INFO VIDEO CENTER

# Sicherheit im PC


## Das Internet

# Das Internet

***Anmerkung :***
Dieses Dokument stammt aus dem Internet. Ich habe es teilweise kopiert und zusammen gefügt. Wenn Sie das Dokument anhand der CD bearbeiten beachten Sie bitte volgendes:
Die Links beziehen sich größtenteils auf das Dokument. Außer bei der Glossary (Erklärungen der Wörter). Diese Links führen sofort ins Internet.
Außerdem werden im Kapitel ***Empfohlene Schutzmaßnahme(n)***
die Links ab ***Punkt 5 E-Mail Sicherheit*** auch ins Internet führen.
Die E-Mail Sicherheit wurde ja schon behandelt und die restlichen Punkte sprengen den Rahmen dieses Seminars.
Der Hauptlink für die Internetseite ist:
**http://www.bsi-fuer-buerger.de/internet/index.htm**

Viel Spaß wünscht Ihnen Oth François

## Inhaltsverzeichnis

# Das Internet

## Internet - was heißt das eigentlich?

Bestimmt wieder irgend etwas Englisches. Naja, nicht ganz. Eigentlich setzt sich das Wort "Internet" aus zwei Teilen zusammen: aus "**inter**" (Latein für "zwischen") und "**net**", der Abkürzung für "networking" (englisch "vernetzen"). Im Rechner-Bereich bedeutet "Internet" deshalb die **Vernetzung zwischen Computernetzen**. Das Internet ist also ein Computernetz-Netz.

Soviel zur Technik. Das Internet ist aber auch das jüngste Massenmedium; Sie können zu fast jedem Thema Informationen finden oder aber selbst einstellen. In Deutschland gibt es derzeit rund **39 Millionen Internetnutzer**, die durchschnittlich mehr als acht Stunden im Monat im Internet sind. Und Sie?

## Wie das Internet entstand

Das Internet ist heute ein weltweites Netzwerk mit Millionen von angeschlossenen Computern, die über Telefon- und Standleitungen, über Satellitenverbindungen und Richtfunkstrecken Daten austauschen. Bevor es aber soweit kam, musste eine Menge passieren.

Wenn man so will, machte Wilhelm Weber mit der Erfindung der elektrischen Telegraphie 1833 den Anfang. In den 30er und 40er Jahren des letzten Jahrhunderts folgte dann die Entwicklung des Computers, ohne den natürlich nichts möglich wäre. Dem Kalten Krieg ist die eigentliche Entwicklung des Internets zu verdanken. Denn der Vorläufer des Internets war das **ARPANET**, welches die USA während des Kalten Krieges entwickelten.

Das US-Verteidigungsministerium gründete 1958 die Forschungsbehörde ARPA (Advanced Research Projects Agency), die mit vielen Forschungseinrichtungen Amerikas zusammen arbeitete. Eine davon war die kalifornische Rand Corporation. Dort entwickelte Paul Baran 1962 ein Konzept über eine Netzwerk-Technologie, die sicherstellen sollte, dass das Kommunikationssystem des U.S. Militärs vor ernsten Zerstörungen durch atomare Angriffe geschützt ist. In seinem Konzept wurden Daten nicht mehr auf einem zentralen Rechner gesammelt, sondern in ein Computernetzwerk eingespeist. Die Daten gelangten über die unterschiedlichsten Verknüpfungen vom Startrechner zum Zielrechner. Dadurch war ein Totalausfall des Netzes kaum mehr zu befürchten. Barans Konzept wurde schließlich umgesetzt und der erste Verbindungsrechner des so genannten ARPANETs wurde am 1.9.1969 an der University of California, Los Angeles (UCLA), in Betrieb genommen. Er bestand aus einem für damalige Verhältnisse leistungsfähigen Minicomputer (Honeywell 516 mit 12 KB Speicher). Robert Kahn und Vinton Cerf entwickelten 1977 ein einheitliches Datenprotokoll und eine Methode der Verbindungsherstellung: **TCP/IP** (Transmission Control Protocol / Internet Protocol). Dieses Übertragungsprotokoll wurde 1983 zum Standard für das ARPANET.

Immer mehr Netze entstanden. 1986 betrieb die **NSF** (National Science Foundation, US-Nationale Wissenschaftsstiftung) NSFNET als **Backbone** für die Verbindung von neuen, regional entstehenden Netzen. **1990** ersetzte das NSFNET schließlich das ARPANET. Darauf folgte die schrittweise Öffnung des Netzes: Immer mehr Personen und Länder, aber auch privat betriebene Netze erhielten einen Zugang zum NSFNET. Die Benutzerzahl stieg stark an. 1991 führte Tim Berners-Lee vom europäischen Kernforschungszentrum **CERN** im Internet ein Hypertextsystem ein. Auf dieser Entwicklung aufsetzend wurde der erste grafische Browser namens **Mosaic** entwickelt, der eine äußerst einfach zu bedienende Benutzeroberfläche hatte. Damit wurden die digitalen Netzwerk-Dokumente nun unkompliziert zugänglich. Mosaic ist deshalb - einfach ausgedrückt - der Vater der Browser. Mit der Einführung des **HTTP** (**H**yper**t**ext **T**ransfer **P**rotocol) waren die grundlegenden Entwicklungen abgeschlossen und das **World Wide Web** war geboren. Dank der Einführung von leicht bedienbaren Browsern wurde das Internet ab **1993** massentauglich.

**Zum Schluss noch die vergangenen zwölf Jahre im Schnelldurchlauf:**

**1992** war die Internetgemeinschaft bereits auf 700.000 Server herangewachsen. Ein Jahr später hatte sich die Anzahl der am Internet angeschlossenen Computer mit 1,8 Millionen mehr als verdoppelt. Hatten bis Mitte der 90er Jahre vorwiegend universitäre Einrichtungen das Netz genutzt, begannen ab

**1994** auch andere Bereiche das Internet zu entdecken. Das Internet wurde erstmals auch **kommerziell** genutzt. Zeitungen stellten einen Teil der Printausgabe online zur Verfügung, die ersten Online-Shops wurden "geboren", zum Beispiel der Online-Buchhändler Amazon.com 1995. Damit kam die **Frage nach der Sicherheit** im Internet auf: Normale Datenübertragung war nicht abhörsicher, also mussten Verschlüsselungstechniken her. Spätestens seit

**1995** redete die ganze Welt dann vom "Cyberspace", vom "Surfen" oder von der "Welt im Netz". Heute gibt es weltweit rund 630 Millionen Internetnutzer.

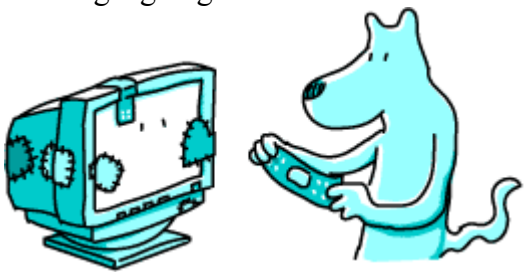
## Der Browser

Internetsurfen ohne Browser ist wie Autofahren ohne Auto - es funktioniert einfach nicht. Mit Hilfe eines Web-Browsers können Sie Daten aus dem weltweiten Netz abrufen und auf Ihrem PC anzeigen und verarbeiten. Die bekanntesten Browser sind Netscape Navigator, Microsoft Internet Explorer, Opera und Mozilla.

Dabei ist der Begriff aus dem Englischen von "**to browse**" abgeleitet und meint soviel wie **durchblättern, schmökern, sich umsehen**. Und eigentlich ist der Name ja auch ziemlich passend ausgewählt. Alles zusammengenommen können Browser eine Vielzahl **unterschiedlicher Medienformate anzeigen und abspielen** und dienen außerdem als **Ablaufumgebung für Programme und Skripte**, den so genannten aktiven Inhalten.

## Der Web-Browser

Mit einem Web-Browser können Sie ganz einfach von einer Internetseite zur nächsten blättern. Denn der Browser interpretiert die Anweisungen für die Übertragung der Seite. Die sind in der **World Wide Web Sprache HTML** - Hyper Text Markup Language - geschrieben. Mit Hilfe der Querverweise im HTML-Format (den so genannten Links) werden die Dokumente im World Wide Web miteinander verknüpft. Dabei hat sich die Browser-Technologie rasant weiterentwickelt. Ursprünglich waren Browser dazu gemacht, **Text und Bilder aus dem Internet zu laden** und anzuzeigen. Mittlerweile können moderne Browser mit Hilfe sogenannter PlugIns, AddOns oder Viewern auch **Graphiken anzeigen**, **E-Mails versenden** und für **Videokonferenzen** und vieles mehr eingesetzt werden.



Genau diese **Vielzahl von Funktionen** bringt jedoch komplexe Konfigurationsmöglichkeiten und potentielle **Sicherheitsprobleme** mit sich. Denn je komplizierter die Browser angelegt sind, desto mehr Fehler können passieren. Solche Programmierfehler werden Bugs genannt. Die Hersteller versuchen die Bugs ständig zu korrigieren und bieten für ihre Produkte sogenannte Patches (engl. Flicken) an, die Sie installieren und damit Ihren Browser zu Hause nachbessern zu können. Dabei ist ein Patch ein Programm, das Funktionen in einem anderen Programm verändert. Dadurch müssen Sie nicht den Browser komplett deinstallieren und wieder neu aufspielen. Manchmal heißen solche "Verbesserungsprogramme" statt Patch auch Update oder Bugfix.

zum Inhaltsverzeichnis

## Datensicherung

Vielleicht haben Sie ja auch schon einmal ein Dokument auf Ihrer Festplatte gesucht, das Sie dringend ausdrucken wollten. Egal ob es die Diplomarbeit, die Steuerunterlagen oder der Homebanking-Beleg war. Aber aus irgendwelchen unerklärlichen Gründen war es auf einmal nicht mehr da. Ihr Computer hatte die Datei einfach so verschluckt, gelöscht oder sonst irgendetwas damit gemacht. Die Datei war jedenfalls weg.
Spätestens seit dieser Situation wissen Sie, dass **gespeicherte Daten auf der Festplatte nicht für alle Zeiten sicher und abrufbar sind**. Deshalb sollten Sie Ihre Daten - auch wenn Sie Ihren PC nur privat nutzen - **regelmäßig sichern**.

Festplatten sind heute sehr zuverlässig. Pannen kann man aber - wie beim Auto - nicht ausschließen, denn die Feinmechanik ist hohen Belastungen ausgesetzt. Die Informationen, dazu zählt auch das, was Sie geschrieben und in einem Datei-Ordner abgelegt haben, werden innerhalb der Festplatte auf magnetisierbaren Scheiben, die zu einem Plattenstapel zusammengefasst sind, gespeichert. Ein solcher Plattenstapel dreht sich in modernen Festplatten mindestens 5.400 mal in der Minute. Oftmals liegt die Umdrehungsgeschwindigkeit bei vielen Modellen sogar noch deutlich höher. Wenn ein Rechner im Laufe eines Jahres nur 100 Stunden arbeitet, hat sich der Festplattenstapel 32.400.000 mal gedreht. Das belastet die Lager. Technische Defekte in diesem Bereich sind zwar selten, kommen aber vor.

Die hohen Umdrehungsgeschwindigkeiten führen zu einem weiteren Problem: Auf Datenträgern wie Disketten oder Festplatten werden die Daten elektromagnetisch gespeichert. Weil die Umdrehungsgeschwindigkeit bei Disketten gering ist, kann der Schreib-/Lesekopf auf der Diskette aufliegen. Anders bei der Festplatte: Würden die Schreib-/Leseköpfe die Oberfläche der magnetischen Scheiben berühren, wären diese durch die hohen Umdrehungszahlen binnen kürzester Zeit zerstört. Ursache dafür wäre die große Reibung. Um zu verhindern dass die Schreib-/Leseköpfe die Scheibe im laufenden Betrieb berühren, schweben sie auf einer hauchdünnen Luftschicht über den Scheiben. Wenn der Rechner allerdings größeren Erschütterungen ausgesetzt wird, kann es passieren, dass die Schreib-/Leseköpfe während des Betriebs auf der Plattenoberfläche aufsetzen. Im Fachjargon wird das als **Headcrash** bezeichnet. Dabei werden kleine Teilchen aus der Oberfläche der betroffenen Scheibe freigesetzt. Die Daten, die an dieser Stelle gespeichert wurden, sind fast immer unwiederbringlich verloren. Es kommt aber noch schlimmer: Manchmal sind die ausgelösten Teilchen größer als die Luftschicht zwischen den Platten und den Schreib-/Leseköpfen. Berühren diese dann die Köpfe, wird die Festplatte noch weiter beschädigt.

Leider gehört gar nicht viel dazu, um eine solche Erschütterung auszulösen. Stöße gegen den Rechner, eine unsanfte Behandlung der Festplatte auf dem Weg zum PC-Händler oder beim Einbau in das Rechnergehäuse können schon ausreichen. Meistens läuft Ihr PC noch eine Weile wie geschmiert, die Schäden machen sich erst nach einiger Zeit bemerkbar.

Damit aber noch nicht genug: Weil die Daten auf Festplatten elektromagnetisch gespeichert werden, können auch starke magnetische Felder, die zum Beispiel in der Nähe von Elektromotoren oder auch Lautsprechern entstehen, Ihre Daten zerstören.

zum Inhaltsverzeichnis

## Viren & andere Tiere

Gefahren lauern überall - auch im Internet. Wer seine Daten nicht schützt, macht es Feinden einfach, diese bei der Übertragung mitzulesen, zu verändern oder sogar zu löschen. Man hört immer öfter von neuen **Viren** oder **Würmern** - Programmen also, die sich selbständig verbreiten oder über E-Mails versandt werden und Schäden auf Ihrem PC anrichten können. Aber auch von **Trojanischen Pferden** ist oft die Rede. Das sind dann Programme, die vom Nutzer unbemerkt sicherheitskritische Funktionen durchführen, indem sie beispielsweise Passwörter abfangen.

Damit ein Virenangriff aber überhaupt stattfinden kann, benötigt das angreifende Programm in irgendeiner Art Zugang zu Ihrem PC - entweder über eine Netzwerk- oder Telefonverbindung oder über Datenträger, wie Disketten oder CD-ROMs.

zum Inhaltsverzeichnis

## Viren



Viren können für Ihren PC manchmal genauso gefährlich sein wie für Sie ein Grippevirus. Viren im Computer funktionieren auch genauso wie Krankheitsviren. Sie zeichnen sich nämlich vor allem durch zwei Sachen aus: Sie können sich selbst verbreiten und richten überall - wo sie sind - Schaden an. Wenn Sie sich einen "harmloseren" Virus eingefangen haben, gibt Ihr Computer vielleicht seltsame Texte aus, oft werden aber Dateien und auch schon mal die ganze Festplatte gelöscht.

- Bis Mitte 2004 waren rund 100.000 unterschiedliche Computer-Viren im Umlauf. Jeden Monat entstehen Hunderte neue.
- Diese haben bislang weltweit Kosten und Schäden in Milliardenhöhe verursacht. Allein in Deutschland ist jährlich von einer dreistelligen Millionensumme auszugehen.
  Und das mit steigender Tendenz.
- Sie stellen aber auch ein gravierendes Sicherheitsproblem dar, wenn vertrauliche Daten unbemerkt weitergeleitet oder Betriebsgeheimnisse ausspioniert werden.

Anstecken kann sich Ihr PC immer dann, wenn Sie **Dateien aus dem Internet auf Ihren Rechner laden**. Viren können aber auch **über Disketten oder CD-ROMs auf Ihren PC gelangen**. In jeder ausführbaren Datei, wie zum Beispiel ***.exe** oder ***.com**, kann sich ein Virus verstecken. Auch Textdokumente vom Typ ***.doc** oder Tabellen vom Typ ***.xls** können virenverseucht sein.

Computer-Viren sind von Menschen geschriebene Programme oder Programmteile. Sie lassen sich nach der Art ihrer Verbreitung in drei Hauptkategorien unterteilen:

**Boot-Viren:**
setzen sich in dem Bereich einer Festplatte oder Diskette fest, der beim Starten eines Computers in den Arbeitsspeicher gelesen wird. Wenn der Prozessor ein Betriebssystem von der Festplatte lädt (= **booten**), egal ob Warm-Start oder Kalt-Start, lädt er deshalb automatisch den Virus. Der erlangt so die Kontrolle über den Rechner.

**Datei-Viren:**
infizieren Programmdateien, wie beispielsweise Betriebssysteme oder Spiele. Wenn der Anwender die befallene Datei startet, infiziert der Virus weitere Dateien und pflanzt sich so fort.

**Makro-Viren:**
können sich auch unabhängig vom eingesetzten Betriebssystem fortpflanzen und sind relativ einfach zu programmieren. Makro-Viren haben sich in den letzten Jahren durch den zunehmenden Datenaustausch per E-Mail und die Nutzung des Internets schlagartig vermehrt.

**Erläuterung**:

Makros sind kleine Programme, die immer wiederkehrende Aufgaben automatisieren, beispielsweise innerhalb von Textverarbeitungsprogrammen. Mittels Makrosprache können aber auch spezielle Benutzerbedürfnisse im Anwendungsprogramm installiert und angepasst werden. Makro-Viren nutzen die Makrosprache eines Anwendungsprogrammes - meistens das Textverarbeitungsprogramm Word für Windows (WinWord). Seine Makrosprache lässt Vorgänge einer Sitzung automatisch und auf "Knopfdruck" ablaufen. Dazu enthält die WinWord-Makrosprache einen an BASIC angelehnten Befehlssatz. Entscheidend für die Verbreitung von Makro-Viren ist die Tatsache, dass die Makros direkt im Dokument gespeichert sind.

In erster Linie wird dabei die Dokumentvorlage NORMAL.DOT infiziert. Weil das Anwendungsprogramm den Virus bei jedem Start neu ausführt, können alle neu angelegten Dokumente mit dem Virus infiziert werden. Und da diese WinWord-Dokumentvorlage standardmäßig von allen WinWord-Dokumenten verwendet wird, kann sich der Virus so optimal verbreiten.

**zum Inhaltsverzeichnis**

## Verbreitungswege

**Virentypen**
Verbreitungswege
**Infektionsarten**
**Virenaufbau**
**Mögliche Schäden durch Computer-Viren**

**Die überwiegende Anzahl der Viren kommen per E-Mail zu Ihrem PC.** Immer weniger Viren gelangen über Diskette oder CD-ROM auf den Computer. Dabei sind auch kommerzielle CD-ROMs nicht grundsätzlich virenfrei - auch auf ihnen können sich infizierte Dateien befinden.

Die meisten Infektionen entstehen durch E-Mail-Würmer. Große Verbreitung finden auch Makro-Viren - vorzugsweise in Office-Dokumenten. Nur wenige werden durch Boot- oder Datei-Viren verursacht. Je höher also die Anzahl der PCs und je mehr davon vernetzt sind, desto schneller können sich Computer-Viren ausbreiten. Da viele **Dokumente als Anhang** mit einer E-Mail verschickt werden, ist die großflächige Streuung der Viren zunehmend einfacher und deshalb tendenziell steigend.

Das Internet ist für Viren auch deshalb attraktiv, weil es weltumspannend ist. Es bietet viele potentielle Infektionsopfer. Außerdem ist das Internet weitgehend unkontrolliert. Programme, die Viren enthalten, können leicht verbreitet werden. Die Viren-Autoren bleiben darüber hinaus noch weitgehend anonym, so dass es schwer ist, diese zu bestrafen.

Dem nicht genug: Seit 1991 existieren Baukästen für die Programmierung von Viren, so genannte **Virus Construction Kits**. Damit kann jeder - auch ohne Fach - oder Programmierkenntnisse - Computer-Viren basteln und in Umlauf bringen.

**zum Inhaltsverzeichnis**

## Infektionsarten

**Virentypen**
**Verbreitungswege**
Infektionsarten
**Virenaufbau**
**Mögliche Schäden durch Computer-Viren**

Es gibt drei Infektionsarten:

- über das Booten
- beim Ausführen eines Programmes (*.exe, *.com, usw.)
- über infizierte Dokumente

**Die Infektionsarten unterscheiden sich in der Art, wie ein Virus sich in einem Programm festsetzt**. Beispielsweise hängen viele Viren ihren eigenen Programmcode an das Ende einer ausführbaren Datei und setzen am Anfang einen Zeiger auf diesen Code. Wird das Programm gestartet, springt es vor der Ausführung seiner eigentlichen

Aufgaben zuerst auf das Virusprogramm. Ist dieses ausgeführt, springt es wieder an die Stelle zurück, an der der Ablauf ursprünglich unterbrochen wurde. Sie merken dann nicht einmal, dass sich das Aufrufen des Programms minimal verzögert hat. Rufen Sie das Programm jetzt auf, startet zuerst der Virus. Er sucht von diesem Moment an nach nicht infizierten, ausführbaren Dateien, um diese auch noch zu befallen.

zum Inhaltsverzeichnis

## Virenaufbau

Virentypen
Verbreitungswege
Infektionsarten
Virenaufbau
Mögliche Schäden durch Computer-Viren

Ein Virus besteht in der Regel aus **drei Programmteilen**:

- Mit dem **Erkennungsteil** stellt der Virus fest, ob die Datei bereits befallen ist. Hierdurch werden unnötige Mehrfachinfektionen vermieden. Der Virus erhöht so seine eigene Ausbreitungsgeschwindigkeit und wird nicht so schnell erkannt.
- Der **Infektionsteil** wählt ein Programm aus und fügt den Programmcode des Virus ein. Das ausgewählte Programm ist nun infiziert und kann von da an selbst bei einem Aufruf weitere Programme infizieren.
- Der **Funktionsteil** legt fest, was im System manipuliert werden soll. Um möglichst nicht gleich entdeckt zu werden, sind in vielen Viren sogenannte "Trigger" eingebaut: Der Virus wird erst aktiv, wenn ein bestimmtes Ereignis eintritt, zum Beispiel an einem bestimmten Datum oder nach dem x-ten Start eines Programms,. Vom einfachen Nichtstun (lediglich Verbreitung) bis zum Löschen der Festplatte ist dabei alles möglich.

Computer-Viren ähneln in ihrer Funktion und ihrem Aufbau sehr Biologischen Viren. Ein Vergleich:

| Biologische Viren | Computerviren |
|---|---|
| Greifen spezielle Körperzellen an. | Greifen auf bestimmte Dateien zu, nämlich Programme (*.exe, *.com, usw. ...) |
| Die Erbinformation einer Zelle wird verändert. | Das infizierte Programm wird verändert. |
| In der befallenen Zelle wachsen neue Viren heran. | Das befallene Programm befällt weitere Programme. |
| Eine infizierte Zelle wird nicht mehrfach vom gleichen Virus befallen. | Fast alle Computer-Viren befallen nur einmal das Programm. |

| | |
|---|---|
| Ein befallener Organismus zeigt unter Umständen lange Zeit keine Krankheitserscheinungen. | Ein befallenes Programm kann auch unter anderem lange Zeit fehlerfrei weiterarbeiten. |
| Viren können mutieren und somit nicht immer eindeutig erkennbar sein. | Manche Computer-Viren können sich verändern und versuchen damit Suchroutinen auszuweichen. |

zum Inhaltsverzeichnis

## Mögliche Schäden durch Computer-Viren



Datei-Viren verändern Programmdateien. Ist ein Programm infiziert, läuft es meistens fehlerfrei. Häufig bemerken Sie eine Infektion nicht sofort, sondern erst später, wenn Sie den Auslöser aktiviert haben.

Ein Beispiel: Der MIX-1 Virus stört das Ausdrucken von Texten und Grafiken auf einem Drucker.

Aus "Sehr geehrte Damen und Herren" wird auf dem Ausdruck dann "Rahr gaahrta Deman ond Harran"

Für Geschäftsbriefe ist dieser Computer damit nicht mehr tauglich. Dieser Virus ist aber noch einer der harmloseren Sorte. Andere können auch sämtliche Kundendaten von Unternehmen löschen. Sind diese Daten nicht vorher gesichert worden, kann das Unternehmen im schlimmsten Fall nicht mehr weiterarbeiten. Noch fataler ist es, wenn Viren die Patientendaten in Krankenhäusern zerstören oder gar ohne dass es jemand merkt verfälschen. Gehen dort Eintragungen über lebenswichtige Medikamente für bestimmte Patienten verloren oder erhalten falsche Werte, ist eine Versorgung dieser Patienten mit diesen Medikamenten nicht mehr gewährleistet.

zum Inhaltsverzeichnis

## Abzocker & Spione

Neben all den "tierischen Gefahren", die Sie im Kapitel "**Viren & andere Tiere**" kennen gelernt haben, gibt es leider noch mehr Gefahren im Internet. Auch die sollten Sie kennen, um sich davor schützen zu können. So wurden die seit 2002 immer stärker verbreiteten **0190-Dialer** bereits für so manchen Internetsurfer zum teuren Spaß. Dieses Unheil bleibt Ihnen erspart, wenn Sie wissen, was Sie tun bzw. nicht tun sollten. Und auch über **Hacker, "Schnüffel-Software" (Spyware) und Massen-E-Mails (Spam)** erfahren Sie hier mehr.

### Dialer

Seit Anfang 2002 schlagen immer mehr Internetnutzer Alarm über überhöhte Telefonrechnungen. Als Grund dafür werden meist die so genannten 0190-Dialer angeführt. Dabei surfen Sie über eine 0190-Nummer, die statt der üblichen zwei bis vier Cent Kosten von bis zu 1,86 Euro (3,63 DM) pro Minute, manchmal sogar über 900 Euro pro Einwahl, verursacht. In vielen Fällen verändern die Wählprogramme sogar dauerhaft die Einstellungen des Computers, so dass alle künftigen Internet-Sitzungen über eine 0190-Nummer laufen.

## *Warum gibt es Dialer?*

Die meisten Internetinhalte sind für Sie kostenfrei. Es gibt aber auch Anbieter, die mit ihren Internetseiten Geld verdienen wollen. Dazu zählen unter anderem Seiten mit erotischen Inhalten, für speziellen PC-Support oder zum Download von Handylogos etc. Natürlich bedarf es dazu eines geeigneten Abrechnungssystems. Kreditkarten wären eine Möglichkeit, sind jedoch aufgrund der relativ hohen Gebühren für kleinere Beträge zu teuer. Außerdem bestünde die Gefahr des Datenmissbrauchs. Bei anderen Zahlungssystemen muss sich der Kunde zuvor anmelden, ein "Spontankauf" ist nicht mehr möglich. Am geeignetsten erscheinen deshalb die bereits im Telefonbereich bewährten so genannten Telefonmehrwertdienste über **0190-Nummern**.

Auch Internetdienste können auf diese Weise abgerechnet werden. Und eigentlich sind 0190-Nummern auch eine praktische Sache: Der Surfer kann im Internet anonym Dienstleistungen nutzen, indem er sich über eine 0190-Nummer einwählt und für die Nutzungsdauer zahlt. Er steuert seine Ausgaben selbst, da er jederzeit die Verbindung trennen kann. Bezahlt wird über die Telefonrechnung. Während die Gebühren für die 0190-Nummern von der Bonner Regulierungsbehörde für Telekommunikation und Post (Reg TP) vorgegeben sind, können die Anbieter der neuen 0190-(0)-Nummern die Preise selbst festlegen - und dabei leider auch hemmungslos abkassieren. Satte 900 Euro für wenige Verbindungssekunden musste schon so mancher ahnungslose Surfer bezahlen. Wie kann das passieren?

**nach oben**

## *So funktioniert ein Dialer*

Damit der Aufbau der kostenpflichtigen Seite erfolgen kann, muss sich der Internetnutzer ein Programm herunterladen. Diese Programme - "Dialer" (= "Einwahlprogramme") genannt - sorgen dafür, dass der Aufbau der Seite über eine

0190-Nummer erfolgt. Bei Windows-Betriebssystemen wird dabei die Installation und Konfiguration der Verbindung ins **DFÜ-Netzwerk** aufgenommen. Die Verbindungskosten sind dann ungleich höher als bei normalen Internetverbindungen. Im Normalfall entscheidet der Nutzer aber selbst, welche Nummer er anwählt. Verlässt er die Internetseite, zahlt er anschließend den ganz normalen Tarif.

Leider gibt es mittlerweile aber eine ganze Reihe von betrügerischen Anbietern, die versuchen, unbemerkt einen solchen Dialer auf fremden Rechnern zu installieren. Diese Dialer-Programme können sich selbständig ins Internet einwählen. Der Surfer merkt in der Regel nicht, dass er sich nicht über seinen regulären **Provider** ins Internet eingewählt hat. Das böse Erwachen kommt Wochen später mit der Telefonrechnung.

**nach oben**

### *Das können Dialer normalerweise nicht*

Im Regelfall haben Dialer bei Ihnen keine Chance, wenn Sie über **DSL** im Internet surfen. Dabei kann sich der Dialer nämlich nicht unbemerkt bei einem fremden Provider einwählen. Doch aufgepasst: Wenn Sie eine DSL-/ISDN-Kombikarte benutzen, geht Ihr Schutz flöten. Dann kann sich ein Dialer unbemerkt einschleichen. Benutzen Sie eine reine DSL-Karte oder einen DSL- oder **ISDN-Router** sind Sie auf der sicheren Seite. Wie bei Viren und Trojanern gilt auch hier: Die meisten sind für das Betriebssystem Windows ausgerichtet. Wenn Sie stattdessen ein anderes verwenden, sind Sie von vorn herein sicherer.

**nach oben**

### *So können Sie sich schützen - Tipps*

So banal es auch klingen mag: Schalten Sie Ihren gesunden Menschenverstand ein! Klicken Sie also gar nicht erst auf Links in Werbe-Mails oder auf den beworbenen Web-Seiten. Installieren Sie keine Programme, die aus unsicheren Quellen stammen. Brechen Sie einen automatisch gestarteten Download sofort ab.

Darauf können Sie außerdem achten:

1. Lassen Sie 0190- Nummern sperren. (Informationen für Telekomkunden unter der kostenfreien Hotline-Rufnummer: 0800-330-1000)
2. Beantragen Sie einen Einzelverbindungsnachweis. Dieser ist für Sie kostenlos.
3. Richten Sie keinen automatischen Internet-Zugang ein! Speichern Sie Ihr Zugangspasswort nicht ab.
4. Installieren Sie ein Dialer-Schutzprogramm, einen so genannten "0190-Warner".
5. Meiden Sie unbekannte Software, E-Mails oder "kostenlose" Dialer.
6. Deaktivieren Sie AktiveX und andere Aktive Inhalte, über die sich Dialer unbemerkt einnisten können.
7. Schalten Sie Ihr - soweit vorhanden - externes Modem ab.
8. Ziehen Sie bei seltener Internet-Nutzung gegebenenfalls das Kabel aus der Telefondose.

9. Wenn Sie über DSL verfügen, so stellen Sie sicher, dass Ihr altes Modem bzw. Ihre ISDN Karte abgeschaltet, ausgebaut oder von der Telefonleitung getrennt sind. Sollte das nicht der Fall sein, könnte ein Dialer Ihre "alte Leitung" missbrauchen.

nach oben

### *Daran erkennen Sie einen Dialer*

Da es sich bei Dialern um legitime Software handelt, werden sie von Virenscannern in der Regel nicht gemeldet. Auch "Firewall"-Software bietet keinen Schutz. Es gibt Programme, die Ihr DFÜ-Netzwerk überwachen und Verbindungen zu 0190-Nummern melden. Die wenigsten dieser Schutzprogramme schaffen es, die Einwahl in allen Fällen zu verhindern, bevor eine Verbindung zustande kommt. Verlassen Sie sich deshalb nicht darauf!

nach oben

zum Inhaltsverzeichnis

Sie sollten auf folgende Punkte achten:

- neue Symbole auf dem Bildschirm
- Modem wählt sich von selbst ein
- Browser hat eine neue Startseite
- 0190-Nummer im DFÜ-Netzwerk
- zu hohe Telefonrechnung enthält den Posten "Servicedienste"

nach oben

### *Das können Sie tun, wenn ein Dialer bei Ihnen aktiv war*

Hat sich trotz aller Vorsichtsmaßnahmen bei Ihnen ein Dialer eingeschlichen, beachten Sie folgende Regeln:

1. **Sichern Sie die Beweise!**

- Internetseite, von der der Dialer stammt
- Bildschirmausdruck der Internetseite
- Dialer auf Diskette oder CD-ROM sichern
- Besitzer der Internetadresse und den Anbieter des Dialers ermitteln (z.B. **www.denic.de**)
- Vollständige 0190-Rufnummer ermitteln

2. **Erstatten Sie Strafanzeige bei der Polizei!**

3. **Erheben Sie Einwände gegen die Telefonrechnung!**
Um die Fristen zu wahren, müssen Sie dem entsprechenden Posten auf der Rechnung Ihres Telekommunikationsanbieters innerhalb von 14 Tagen schriftlich widersprechen.

4. **Holen Sie sich rechtlichen Rat ein!**
- zum Beispiel beim Verein "Freiwillige Selbstkontrolle Telefonmehrwertdienste e.V." (**www.fst-ev.org**)

**nach oben**

### *Schon von 0900-Nummern gehört?*

Seit dem 1. Januar 2003 gibt es neben den 0190-Nummern auch die 0900-Nummern als weitere so genannte Premium-Rate-Dienste. Ziel der 0900- Nummern ist es, die 0190-Nummern bis Ende 2005 abzulösen, um den europäischen Telefonmarkt einheitlicher zu machen.

Wie bei den 0190-0-Nummern und den Vorwahlen 0191, 0192, 0193 gibt es bei den 0900-Nummern **kein festes Tarifschema**. Der Anbieter einer solchen Nummer kann die Kosten derzeit ohne feste Obergrenze völlig frei festlegen. Die neuen Nummern bieten aber auch Vorteile: Der Anbieter dieses Premium-Rate-Dienstes ist nicht anonym und kann bei Missbrauch ermittelt werden. Zusätzlich werden die Nummern in Kategorien unterteilt, die dem Anwender die Art des Dienstes anzeigen soll. Diese Einteilung ist für den Betreiber allerdings freiwillig und damit nicht verpflichtend. Die Nummern sind **folgenden Angeboten** zugeordnet:

- 0900-1 Informationsdienste
- 0900-3 Unterhaltungsdienste
- 0900-5 "sonstige Dienste" (d.h. auch Erotikangebote)
- 0900-9 Dialer

Die deutsche Telekom versucht, den Verbraucher bei den neuen Nummern besser zu schützen. Es wurde eine Obergrenze von 2,50 € pro Minute bei Blocktarifen von 5 € pro Minute festgelegt. Jeder höhere Betrag muss vom Kunden durch einen Tastendruck bestätigt werden. Zusätzlich ist es für alle Netzbetreiber Pflicht, bestehende Verbindungen nach 60 Minuten zu unterbrechen. Hierdurch sollen unnötig hohe Rechnungen vermieden werden. Vom Mobiltelefon sind die neuen Nummern vorerst noch nicht erreichbar. Hier ist die Rechnungslegung noch nicht geklärt.

Die 0900-Nummern erreichen Sie nicht nur über Ihr Telefon, sondern auch über den PC. Den schützen Sie vor unliebsamen Überraschungen am besten, indem Sie Ihre **Anti-Dialer-Software um den Eintrag "0900" erweitern**. Ein solches Programm finden Sie auch in unserer **Toolbox**.

**nach oben**

### *Die Gesetzeslage*

Anfang März 2004 hat der Bundesgerichtshof ein entscheidendes Dialer-Urteil gefällt. Danach müssen unbemerkt entstandene Dialer-Kosten nun nicht mehr bezahlt werden. Voraussetzung ist, dass die Anwahl zu der teuren Nummer über einen heimlich im Computer des Geschädigten installierten Dialer erfolgte. Der Kunde muss dann nur die Standard-Verbindungskosten bezahlen. Dieses Urteil ändert die bisherige Rechtslage erheblich - zugunsten des Verbrauchers.

Wenige Monate zuvor war das Gesetz zur Bekämpfung des Missbrauchs von 0190er und 0900er-Mehrwertdiensterufnummern in Kraft getreten.

Die wichtigsten Regelungen:

1. **Einfache Ermittlung des Anbieters einer (0)190er Rufnummer**
Sie haben von nun an einen Auskunftsanspruch gegenüber der Regulierungsbehörde für **Telekommunikation und Post** (RegTP) und können die Herausgabe von Namen und Anschrift der Anbieter fordern. Die Anbieter wiederum sind verpflichtet, vor Beginn der kostenpflichtigen Verbindung auf den Preis des Telefonates hinzuweisen.

2. **Maximale Entgelte**
Einwahlen für mehrere Hundert Euro sind nun tabu: Für eine Verbindung darf nur noch ein Entgelt von maximal zwei Euro pro Minute erhoben werden. Bei Blocktarifen, d.h. zeitunabhängigen Dienstleistungen / pro Anruf, liegt die Obergrenze bei 30 Euro pro Einwahl. Nach spätestens einer Stunde muss die Verbindung automatisch getrennt werden.


3. **Dialer werden registriert**
Neu ist auch das Registrierungsverfahren für Dialer. Sie müssen nun - im Sinne des Verbraucherschutzes - bestimmte Mindestvoraussetzungen erfüllen. Darüber hinaus sind Internet-Dialer auf eine einzige Rufnummerngasse beschränkt, das heißt die Vorwahl ist auf 0900-9 festgelegt. Das macht es für Sie einfacher, diese Nummernfolge sperren zu lassen. Die RegTP hat dank dem neuen Gesetz die Befugnis, die Nummern bei rechtswidrigem Missbrauch zu entziehen.

"Kostenpflichtige Dialer dürfen ab dem 14. Dezember 2003 nur noch über die Rufnummerngasse 0900-9 betrieben werden. Darauf weist die Regulierungsbehörde für Telekommunikation und Post (Reg TP) ausdrücklich hin."
Weitere Einzelheiten unter: **www.regtp.de/aktuelles/pm/02878/index.html**

Mit dem neuen **Gesetz** gehören die spektakulären Fälle, in denen Dialer fast 5000 Euro pro Stunde oder 900 Euro pro Einwahl abzockten, der Vergangenheit an. Als Verbraucher sind Sie jetzt auf jeden Fall besser geschützt. **Trotzdem gilt: Wachsam bleiben!**

**nach oben**

## Infiziert - und nun?

Rund 60 Prozent der Surfer in Deutschland hatten bereits Probleme mit **Computer-Viren oder Würmern**. Auf rund 85 Prozent der PCs ist deshalb inzwischen eine **Anti-Viren-Software** installiert. Trotz allen Vorsichtsmaßnahmen kann es passieren, dass es Sie trotzdem erwischt. Und dann?

## Schützen - aber wie?

Ohne Frage - für Ihre Sicherheit müssen Sie etwas tun. Aber der Aufwand lohnt sich. Denn wer rechtzeitig vorsorgt und seine Daten schützt (und regelmäßig sichert) reduziert das Schadensrisiko erheblich. Diese Vorsorge kann Ihnen Zeit, Geld und Nerven ersparen. Die bräuchten Sie nämlich ganz sicher, wenn der Schaden erst einmal da ist.

**Wieviel Aufwand** Sie betreiben müssen, hängt - wie immer - von Ihren **persönlichen Anforderungen** ab. Und selbst wer jetzt denkt: "Welche Informationen sollen auf meinem PC schon zu holen sein..." - auch der ist hier genau richtig. Denn auch für den gilt: Fast jeder besitzt Informationen, die in die falschen Hände gelangen könnten.

Um das zu verhindern kommt es besonders auf **zwei Dinge** an: Erstens sollten Sie Ihren eigenen PC (bestimmte Anwendungen und ausgewählte Informationen) mittels Passwörter schützen und zweitens Daten, die übertragen werden müssen, verschlüsseln. Mehr Informationen zum richtigen Umgang mit Passwörtern und zur Datenverschlüsselung finden Sie auf den folgenden Seiten. Los geht's aber zunächst mit der Frage "Wer braucht welchen Schutz?" und einem **Überblick** über die wichtigsten Schutzmaßnahmen.

## Wer braucht welchen Schutz?

Ganz egal ob Sie Ihren PC für Computerspiele, zum Surfen oder auch für den Beruf nutzen **- Sicherheit** brauchen Sie in jedem Fall. Aber warum mehr machen als unbedingt nötig?!
Es lohnt sich zu überlegen, **welchen Schutz** Sie genau benötigen. Die nachfolgende Tabelle zeigt Ihnen die wichtigsten PC-Nutzungsarten. Ein kurzer Blick - und Sie wissen, welche Schutzmaßnahmen Sie vornehmen sollten und wo es ausführlichere Informationen dazu gibt.

| PC-Nutzung: | Empfohlene Schutzmaßnahme(n): | Zusatz-informationen: |
|---|---|---|
| nur Spiele offline | 1 | |
| einfache private Nutzung, Textverarbeitung | 1; 2 | |
| Internet | 1 bis 6 | |
| Online-Banking | 1 bis 8 | |
| Berufliche Nutzung + Online-Banking | 1 bis 12 | **Leitfaden IT-Sicherheit** |
| Kinder | 13; 14 | |

Empfohlene Schutzmaßnahme(n):

1. **Virenschutz**
2. **Datensicherung**
3. **Patches und Updates einspielen**
4. **Personal Firewall**
5. **E-Mail-Sicherheit**
6. **Browser-Sicherheit**
7. **Sorgfältig mit PIN/TAN umgehen**
8. Verschlüsselt mit Bank-Server kommunizieren
9. Überspannungsschutz an der Steckdose
10. **Trennung von Nutzungsbereichen**
11. **Vertrauliche Daten verschlüsselt speichern**
12. Ggf. Support-Vertrag abschließen
13. **Zugangsschutz am Rechner**
14. **Kinderschutzsoftware**

zu 10.: Wenn mehrere Benutzer einen PC verwenden, sollte jeder ein eigenes Benutzerkonto haben. Das ist bei fast allen Betriebssystemen möglich. Und auch Spiele und Arbeit sollten voneinander getrennt sein. Diese Trennung erreichen Sie, indem Sie verschiedene Betriebssystempartitionen einrichten. Beim Hochfahren des Computers können Sie dann mit dem "Bootmanager" eine dieser Partitionen auswählen. Falls Sie ohnehin mehr als einen Computer besitzen, können Sie natürlich auch einfach auf dem einen Computer spielen und auf dem anderen arbeiten.
**nach oben**

**Firewall**
Personal Firewall
Online-Virenscanner
Proxy-Server

## *Firewall*

Die Aufgabe einer Firewall ist so ähnlich wie die einer Brandschutzmauer bei Häusern, deshalb heißt sie wohl auch so.
Die Firewall (deutsch "Brandschutzmauer") besteht aus Hard- und Software, die den **Datenfluss zwischen dem internen Netzwerk und dem externen Netzwerk kontrolliert**. Alle Daten, die das Netz verlassen werden ebenso überprüft, wie die, die hinein wollen.

Firewalls werden in der Regel von Unternehmen eingesetzt. Schließlich ist es da ganz besonders wichtig, dass die Computer nicht ungeschützt mit dem Internet verbunden sind. Mit Hilfe der Firewall müssen die Firmen nicht jeden einzelnen Arbeitsplatzrechner absichern, sondern nur die Rechner und Server, die unmittelbar an das externe Netzwerk angeschlossen sind. Diese Rechner werden so konfiguriert, dass sie die sie passierenden Daten kontrollieren können. Die Firewall **überprüft** beispielsweise anhand der IP-Adresse des Rechners, ob das Datenpaket, das ins Netzwerk hinein will, überhaupt dazu berechtigt ist. Der Firewall-Administrator legt dafür Listen mit erlaubten Sendern (Adressen) an. Nur die Daten dieser Sender dürfen die Mauer passieren. nach oben

Firewall
**Personal Firewall**
Online-Virenscanner
Proxy-Server

## *Personal Firewall*

Im Prinzip haben die Firewall und die für den Privatgebrauch abgespeckte Version der Personal Firewall nicht mehr viel gemeinsam. Denn während bei der normalen Firewall viele Rechner durch einzelne ausgewählte geschützt werden, versucht sich der PC bei der Personal Firewall selbst zu schützen. Wie es der Name schon sagt, läuft die Personal Firewall auf dem PC selbst. Sie soll genau wie die normale Firewall den Rechner vor Angriffen von außen schützen und auch verhindern, dass bestimmte Programme, zum Beispiel so genannte Spyware, Kontakt vom Rechner zum Internet aufnimmt. Dazu kontrolliert sie alle Verbindungen in andere Netzwerke und überprüft sowohl die Anfragen ins Internet als auch die Daten, die zum Rechner kommen.

Eine Personal Firewall verfügt in der Regel **folgende Funktionalitäten**:

• **Paket Filter**: Dieser kontrolliert, ob die Daten der an- und ausgehenden Pakete auch dem vom Benutzer festgelegten Regeln entsprechen.

• **Sandboxing**: Dabei werden einzelne Programme in eine eingeschränkte Umgebung "gesperrt". In diesem implementierten Schutzbereich werden Programme ausgeführt. Falls es sich dabei um Schadsoftware handeln sollte, kann sie aber keinen Schaden anrichten, da durch die Isolation der Rest des Systems davon nicht beeinflusst wird.

Wie für jedes Programm ist auch hier entscheidend, wie Sie die Firewall bei der Installation konfigurieren:

- Definieren Sie die Filterregeln so, dass nur die unbedingt notwendigen Zugriffe erlaubt sind.
- Überprüfen Sie die Einstellungen regelmäßig.
- Sperren Sie nicht benötigte **Ports**.

Um die Warnungen Ihrer Firewall zu verstehen, sollten Sie die Bedeutung von IP-Adressen und Host-/Rechnernamen sowie die gemeldeten Ports kennen.

Manche Personal Firewalls beinhalten eine **selbstlernende Konfiguration**. Dabei baut sich die Firewall mit der Zeit ein eigenes Regelwerk auf. Für den technischen Laien ist das ziemlich bequem. Es birgt aber auch das Risiko, dass sich schnell sicherheitskritische Fehlkonfigurationen einschleichen können.

Über Sinn und Unsinn von Personal Firewalls streiten sich die Fachleute noch immer. Denn Desktop Firewalls - wie sie auch genannt werden - sind, wenn man sich an die wichtigsten Grundregeln zum sicheren Surfen hält, fast überflüssig. Wichtig ist, dass das Betriebssystem, der Browser, der E-Mail-Client und die Anwendungen so sicher wie möglich konfiguriert sind. Solange das der Fall ist, Sie nichts aus unsicheren Quellen herunterladen und auch sonst vorsichtig im Internet unterwegs sind, stellt eine Personal Firewall nicht unbedingt einen zusätzlichen Schutz dar.

**Generell gilt:** IT-Sicherheit kann nicht durch eine einzelne Software erreicht werden, sondern ist immer nur durch ein Zusammenspiel von verschiedenen Faktoren möglich.

Und alle, die es jetzt genauer wissen wollen, finden eine Personal Firewall in der **Toolbox**.

**nach oben**

### *Online-Virenscanner*

Manche Privatanwender sehen Online-Virenscanner als Alternative zu herkömmlichen Antiviren-Programmen an. Auf den ersten Blick ist das auch logisch: Weil der Virenscanner direkt über das Internet ausgeführt wird, erspart man sich die Installation eines vollständigen Antiviren-Programms. Und zusätzlich muss man sich auch nicht ständig um die Aktualisierung der **Virensignaturen** kümmern, da online immer die neuesten Updates zur Verfügung gestellt werden. Doch weil Bequemlichkeit eben nicht alles ist, reicht das allein nicht aus, um ein vollständiges Antiviren-Paket ersetzen zu können.

Denn setzen Sie auf Ihrem PC allein einen Online-Scanner als Schutz ein, fehlt Ihnen der Hintergrund-Wächter. Das ist eine Funktion, die bei den herkömmlichen Antiviren-Programmen jede auf dem Rechner angefasste Datei prüft. Um einen ähnlichen Effekt bei einem Online-Virenscanner zu erzielen, müsste man ständig seinen Rechner bzw. die neu hinzukommenden Dateien durch den Online-Scanner überprüfen lassen. Und deshalb ist der Vorteil, dass man sich nicht mehr um die neuesten Virensignaturen kümmern muss, auch nichts mehr wert.

Doch damit nicht genug. Online-Virenscanner haben noch **zwei weitere Nachteile**:

- Sie setzen voraus, dass man **ActiveX** aktiviert hat. Generell sollte man ActiveX im Browser soweit es möglich ist vermeiden, denn es enthält keinerlei Schutzmechanismen. (siehe **Aktive Inhalte**)
- Wenn Sie den konkreten Verdacht haben, dass Ihr PC bereits infiziert ist, sollten Sie die Internetnutzung weitestgehend vermeiden. Denn über jede Online-Verbindung verbreitet sich der Schädling noch weiter. Und falls Sie sich einen **Dialer** eingefangen haben, wählen Sie sich im schlimmsten Fall auch noch über eine teure 0190-Nummer ins Internet ein.

Könnte Ihnen einen Online-Virenscanner trotz aller Nachteile dennoch nützlich sein? Ja, wenn Ihr Rechner bislang ungeschützt ist und Sie den Verdacht haben, dass sich ein Virus auf Ihrem Rechner befindet. Beim Aufspüren des Schädlings kann Ihnen der Online-Scanner behilflich sein. Zu diesem Zeitpunkt kann der Virus allerdings schon einen irreparablen Schaden angerichtet haben. Deshalb sollten Sie nach der Beseitigung des Schädlings zukünftig auf ein **herkömmliches Antiviren-Programm** zurückgreifen. Oberstes Gebot dafür ist, die Virensignaturen immer auf dem neuesten Stand zu halten.

**nach oben**

**Firewall**
**Personal Firewall**
**Online-Virenscanner**
**Proxy-Server**

### *Proxy-Server*

In diesem Zusammenhang hört man auch oft den Begriff "Proxy-Server". Er **kann Bestandteil einer Firewall sein**. Eigentlich ist ein Proxy-Server (z. B. für das WWW) ein Rechner, der Internet-Seiten, die von den WWW-Nutzern häufig abgefragt werden, zwischenspeichert. Wenn der Surfer eine Webseite anwählt, prüft der Proxy-Server, ob ihm die Daten bereits vorliegen. Ist das der Fall, bekommen der Surfer nur eine **"Kopie"**, die schneller übertragen werden kann als das "Original". Sind die Daten jedoch noch nicht vorhanden, lädt der Proxy-Server die entsprechende Seite, speichert sie selbst (im so genannten Cache) und sendet sie dem Surfer. Im Normalfall merkt der Surfer gar nicht, von wo die Daten kommen. Während normalerweise ein Proxy-Server lediglich den Zweck hat, die Zugriffe auf die abgerufenen Seiten zu beschleunigen, erfüllt er in einer Firewall-Anordnung die Aufgabe, zu kontrollieren, ob die übertragenen Daten auch so sind, wie sie sein sollen. Es ist auch möglich, bestimmte Teile nicht zu übertragen. **Aktive Inhalte** in Web-Seiten können so beispielsweise schon in der Firewall blockiert werden.

**zum Inhaltsverzeichnis**