Quelle: http://www.bsi-fuer-buerger.de/01/

Das Internet

Internet - was heißt das eigentlich? Bestimmt wieder irgendetwas 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 **27 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** (**A**dvanced **R**esearch **P**rojects **A**gency), 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** (**N**ational **S**cience **F**oundation, 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 grafische 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 zehn 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 580 Millionen Internetnutzer. Im Jahr 2005 soll die Milliardenschwelle überschritten werden.

Wie das Internet funktioniert

Das Internet ist ein weltweiter Verbund von Rechnern - soviel wissen Sie schon. Der Datenaustausch zwischen den einzelnen Computern ist über gemeinsame Standards, so genannte Protokolle, geregelt. So ist sichergestellt, dass ein Rechner den anderen "versteht". Kommunizieren zwei Rechner über die so genannten **Netzwerkprotokolle**, werden dabei verschiedene Informationen ausgetauscht. Zum Beispiel kann ein Computer über das Protokoll Informationen über sich selbst schicken und sich damit beim anderen Computer identifizieren. Der angewählte Computer kann dann entscheiden, ob er überhaupt Daten austauschen möchte.

Beim Datenaustausch gibt es immer einen, der Informationen gibt und einen, der sie empfängt. Der anbietende Computer wird **Server** (engl. "to serve"= dienen, versorgen) genannt, der nehmende heißt **Client** (Kunde). Der Client schickt Anfragen des Benutzers mit Hilfe eines speziellen Protokolls an den Server. Dessen Antworten stellt er dann in einer für den Menschen verständlichen Weise auf dem Bildschirm dar. Damit die beiden aber überhaupt Informationen austauschen können, muss eine Verbindung zwischen ihnen hergestellt werden.

Über einen **Provider** wählen Sie sich ins Internet ein. Sie müssen beim Provider dafür bezahlen, dass er Ihnen den Zugang zum Internet über seinen eigenen Internet-Server zur Verfügung stellt. Die in Deutschland bekanntesten Provider sind T-Online und AOL.

Zusammengefasst heißt das: Der Provider ist die Schnittstelle zwischen Ihnen - also dem Anwender - und dem Netz. Und ob sich bei Ihnen zu Hause die Internetseiten schnell oder langsam aufbauen, liegt oft an der Kapazität des Providers, daran wie viele Leitungen er den Benutzern zum Surfen im Internet zur Verfügung stellen kann. Wenn es also Sonntag Nachmittag draußen regnet und jedermann Zeit zum Surfen hat, dann kann das mit dem Seitenaufbau im Netz ein wenig länger dauern.

Apropos Netz. Wie entsteht überhaupt so ein Netz?

Wenn Sie per Computer Daten mit jemanden austauschen wollen, so funktioniert das beispielsweise, indem Sie eine Diskette mit Informationen von einem zum anderen PC bringen. Auf Dauer ist das allerdings zu umständlich. Um weiter entfernte Computer direkt miteinander zu verbinden, benötigen Sie in der Regel ein **Modem (oder ISDN-Karte) und eine Telefonleitung**. Die Rechner können nun ganz schnell und einfach Daten tauschen. Allerdings hat die Sache einen Haken: Während die PCs miteinander kommunizieren, ist bei Ihnen Sendepause, denn Ihr Telefonanschluss ist besetzt. Das war in der Vergangenheit für viele sehr ärgerlich. Also baute man separate Netze da auf, wo viele Daten ausgetauscht werden, zum Beispiel in Universitäten oder Unternehmen. Solche lokalen Netzwerke wurden **L**ocal **A**rea **N**etwork - kurz **LAN** - genannt. Damit die Rechner der Universität aber auch mit anderen Rechnern Daten austauschen konnten, schloss man die LANs zu einem Netzwerk mit Hilfe externer Knotenrechner zusammen. Das hieß dann **W**ide **A**rea **N**etwork - kurz **WAN**.

Das Internet ist demnach kein einheitliches Netzwerk, sondern ein **Verbund aus vielen kleinen, geographisch oder organisatorisch begrenzten Netzen** und damit ein dezentrales Netzwerk. Deshalb gibt es auch keinen einzigen "Superrechner", der das Internet steuert, sondern viele Hunderttausende. Sie sind miteinander verknüpft und

damit gewissermaßen das Rückgrat des Internets. Darum heißen die breitbandigen Hauptstrecken des Internets auch so: Backbone. Diese Leitungen tragen die Hauptlast des Datenverkehrs.

Weil es ein einheitliches Internet nicht gibt, braucht man Regeln, die den Datenaustausch zwischen den vielen weltweiten Netzen festlegen. Dadurch entstehen - wie in unserer Gesellschaft auch - Hierarchien. Die großen Knotenrechner sind zum Beispiel dafür zuständig, den Datenverkehr zwischen unterschiedlichen Netzwerken zu regeln.

Internetdienste

Sie können als Anwender im Internet verschiedene Dienste nutzen. Zwei der wichtigsten Dienste sind das **World Wide Web** und **E-Mail**. Nanu, denken Sie vielleicht jetzt: Internet und WWW ist nicht das gleiche? Nein, Internet ist der Oberbegriff für die vernetzten Computernetze einschließlich der angebotenen Dienste. Wenn heute vom Internet geredet wird, dann ist meist aber - fälschlicherweise - das **W**orld **W**ide **W**eb (**WWW**) gemeint.

World Wide Web
Das WWW ist eigentlich nichts anderes als eine multimediale Anwenderoberfläche, die verteilte Dokumente miteinander vernetzt. Mit Hilfe von Links können Sie von Begriff zu Begriff, von Dokument zu Dokument springen. Das WWW bietet Ihnen weltweit Informationen unterschiedlicher Art: Texte, Bilder, Grafiken, Klänge, Videos. Fast das gesamte digitalisierte Wissen der Menschheit ist über Webseiten erreichbar. Und täglich kommen hunderttausende Seiten dazu. Printmedien (Verlage) (gedruckte Publikationen), Universitäten, Museen, nationale und internationale Organisationen, Vereine, Unternehmen, Privatpersonen und viele andere mehr bieten unzählige Informationen. Jede Webseite hat eine **Adresse, die so genannte URL**, und kann über einen Browser aufgerufen werden. Im World Wide Web (WWW) wird die Dokumentensprache Hyper Text Markup Language (HTML) verwendet. Damit können Querverweise (Links) zu anderen Dokumenten hergestellt werden, sowie beliebig viele Bilder, Filme oder Audiodaten in ein Dokument eingebunden werden. Die HTML-Daten werden mit Hilfe des Kommunikationsprotokolls HTTP (Hypertext Transfer Protocol) zwischen dem Web-Server und Ihrem Browser übertragen.

E-Mail:
E-Mail steht für "**electronic mail**" ("elektronische Post") und ist wahrscheinlich der meistgenutzte Dienst des Internets. Dank E-Mail müssen Sie Ihre Briefe nicht mehr mit Papier und Bleistift schreiben, sondern können Ihre Nachrichten mit der Tastatur verfassen. Es gibt auch keinen Briefträger, der den Brief übermittelt. Das erledigen die Leitungen des Internets für Sie. Neben Texten können Sie mit diesem Dienst auch Bilder, Grafiken, Videos, Klänge, Programme oder eine Kombination daraus verschicken. Innerhalb kürzester Zeit kann so eine Nachricht an jeden beliebigen Punkt der Erde gesendet werden.

Technisch gesehen ist das mit dem E-Mail-Schreiben schnell erzählt: Um E-Mails versenden zu können, benötigen Sie entweder ein spezielles Programm, den so genannten "**Mail-Client**" (z. B. Microsoft Outlook, KMail, Lotus Notes), der bei den meisten Betriebssystemen dabei ist. Oder Sie nutzen eine **E-Mail-Web-Schnittstelle** (z. B. bei web.de oder GMX). In jedem Fall brauchen Sie aber ein Postfach, das Ihnen Ihr Provider in der Regel kostenlos einrichtet (z. B. susi.ahnungslos@t-online.de). Wenn Sie jemandem schreiben wollen, müssen Sie die E-Mail-Adresse des Empfängers kennen. Sie schicken Ihre Nachricht dann an dessen Postfach. Der E-Mail-Empfänger muss nicht zum gleichen Zeitpunkt online sein, sondern kann Ihre Nachricht abrufen, wenn er wieder im Internet ist. Entweder lädt er sie über den Mail-Client direkt auf seinen Computer oder er benutzt die WWW-Seite seines (E-Mail-) Providers und liest seine E-Mails dort.

Noch ein Hinweis zum Schluss: Eine oder mehrere Empfänger-Adressen tragen Sie normalerweise im Eingabefeld "An" ein. Wollen Sie bestimmte Personen nur über die E-Mail informieren, sie aber nicht direkt ansprechen, so können Sie das Eingabefeld "Cc" ("Carbon copy": Durchschlag) verwenden. Alle "An"- und "Cc"-Empfänger sehen in Ihren E-Mails auch die anderen "An"- und "Cc"-Empfänger. Zusätzlich gibt es das Eingabefeld "Bcc" ("Blind carbon copy" - Blinddurchschlag). Das benutzen Sie, wenn Sie eine E-Mail an solche Empfänger versenden wollen, die von allen anderen Empfängern nicht gesehen werden sollen. Der "Bcc"-Empfänger selbst sieht alle Adressaten, außer denjenigen, die diese E-Mail ebenfalls per "Bcc" erhalten haben.

Weitere Dienste
Neben E-Mail und dem WWW gibt es viele weitere nützliche Internetdienste, die man in der Regel auch über einen WWW-Browser nutzen kann. Dies sind zum Beispiel **FTP**, **Telnet**, und **Usenet**:
FTP ("file transfer protocol" - Datenübertragungsprotokoll) bietet die Möglichkeit, auch große Dateien zu übermitteln.
Mit Hilfe von Telnet loggt man sich auf einem entfernten Rechner ein, um auf diesem zu arbeiten.
Und Usenet meint die Gesamtheit aller Newsgroups, also die schwarzen Bretter im Internet.

Wie das Internet organisiert ist

Im Internet gibt es Millionen Computer. Die Schwierigkeit ist, diese so zu verwalten, dass jeder einzelne in Sekundenbruchteilen gefunden werden kann. Deshalb gibt es ein System:

Jeder einzelne Computer ist im Internet durch eine **IP-Nummer** oder IP-Adresse eindeutig identifizierbar. Eine IP-Adresse besteht aus 4 Zahlen zwischen 0 und 255 (z.B. 194.95.179.205). Weil sich Menschen diese Zahlenadressen meistens nur schwer merken können, wurden sie in Namensadressen übersetzt. Sie können also entweder die Zahlenadresse oder die Namensadresse verwenden. Diese Internetnamen werden von verschiedenen Organisationen vergeben.

Jeder Name kann weltweit nur einmal vergeben werden.

Das ganze sieht dann beispielsweise so aus:

	http://	**www.bund.de**	
Das **Protokoll**:	http		
Der **Rechnername**:		www	.bund .de
Die **Domain**:			.bund .de
Die **Top-Level-Domain**:			.de

Oder Sie geben die IP-Nummer ein : 194.95.179.205

Um auf eine bestimmte Seite innerhalb von **www.bund.de** zu gelangen, müssen Sie dann noch den konkreten Pfad angeben.
Der könnte zum Beispiel "**Bundeslaender/Berlin-.5305.htm**" heißen. Die komplette Adresse lautet dann: **http://www.bund.de/Bundeslaender/Berlin-.5305.htm**

Die **Top-Level-Domain** kann sich einerseits auf das Land beziehen z.B.

.de	für Deutschland
.it	für Italien
.es	für Spanien

Zusätzlich zu den Länderkennungen gibt es aber auch noch eine Unterteilung nach den **Inhalten**, z.B.

.com	für kommerzielle Zwecke, Unternehmen
.edu	für Bildungseinrichtungen
.org	für nichtkommerzielle Organisationen
.info	allgemeine Infos

Wenn Sie auf Ihrem Rechner eine Internetseite aufrufen, dann schickt der absendende Computer die Informationen nicht als ganzes Stück. Die Daten werden vielmehr **in Datenpakete zerlegt**, einzeln adressiert und machen sich dann auf verschiedenen Routen von Knotenrechner zu Knotenrechner quer durch die ganze Welt auf den Weg zu Ihnen. Anschließend werden die Informationen auf Ihrem PC wieder zusammengesetzt. Dabei kann es passieren, dass eine Nachricht von München nach Stuttgart einen Umweg über New York macht. Durch die neuen Satellitenanbindungen ist sogar ein Umweg durchs Weltall möglich. Sie als Internetsurfer merken davon aber nichts. Nur, wenn zu viele Benutzer auf die Leitungen zugreifen, kann es passieren, dass die Informationen nur sehr langsam bei Ihnen eintröpfeln oder die Übertragung

sogar vollständig zusammenbricht.

Quelle: http://www.bsi-fuer-buerger.de/02/

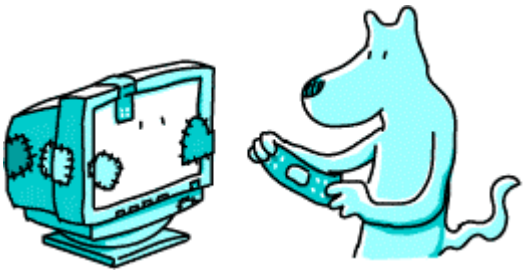
Der Browser

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 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, dass 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.

Aktive Inhalte

Wenn Sie die Grundeinstellung Ihres Browsers unverändert lassen, erlauben diese

meist die Ausführung unbekannter Codes, die in die Informationsangebote der Server-Betreiber eingebunden sind. Diese Programme oder Scripte werden auf Ihren Rechner heruntergeladen. Sie als Benutzer haben dabei keinerlei Kontrolle darüber, was die Programme eigentlich auf Ihrem PC anstellen.

Solche Programme oder Scripte werden als aktive Inhalte bezeichnet und sind meist mit den Programmiersprachen Java, JavaScript oder ActiveX erstellt.

Java und Java-Applets

Java ist eine **universelle Programmiersprache**, die sich besonders **für Internetanwendungen** eignet. Sie wurde von der Firma Sun Microsystems entwickelt - ursprünglich zur Steuerung von Haushaltsgeräten. Java bietet die Möglichkeit HTML-Dokumente mit Spezialeffekten auszustatten, zum Beispiel 3-D-Modellen. Mit Java können sowohl eigenständige Anwendungen als auch Internetanwendungen erstellt werden. Solche Internetanwendungen werden Java-Applets genannt und sind rudimentäre Programme, die von einem Server heruntergeladen und auf Ihrem PC ausgeführt werden. Zur Ausführung von Java-Programmen wird eine "Java Virtual Machine" benötigt. Diese ist heute in den verbreiteten Browsern eingebaut. Damit lassen sich Java-Applets auf nahezu jedem Computer, unabhängig von dessen Hardware oder Betriebssystem ausführen - also im Prinzip auch auf Fernsehern, Waschmaschinen und Telefonen.

Wenn Sie also eine Internetseite anschauen möchten, auf der Java-Applets verwendet werden, dann werden die Programme automatisch auf Ihren PC geladen. Sie laufen dann in der Regel ohne Zugriff auf die restlichen Dateien auf Ihrem Rechner ab. Manchmal passieren bei der Implementierung der Java Virtual Machine aber auch Fehler. Die Java-Applets haben dann doch Zugriff auf die Dateien auf Ihrem PC. Durch diese **Sicherheitslücken** ist es einem arglistigen Dritten zum Beispiel möglich, **Sitzungsinformationen über Sie aufzuzeichnen**. Er weiß dann ganz genau, welche Internetseiten Sie sich angesehen haben. Unter Umständen erhält er so auch Zugriff auf Benutzernamen, Passwörter oder Kreditkartennummern.

JavaScript

JavaScript hat **technisch wenig bis gar nichts mit Java gemeinsam**. Den Begriff gibt es nur, weil bei der Einführung von JavaScript "Java" in aller Munde war. JavaScript eignet sich besonders zur Überprüfung von Formulareingaben. Man kann Berechnungen durchführen, Laufschriften anzeigen und einige technische Daten über den jeweiligen Computer ermitteln.

JavaScript wurde von der Firma Netscape entwickelt und wird direkt vom Browser

interpretiert und ausgeführt. Ein JavaScript-Code kann vom Browser interpretiert werden, ohne dass er vorher in ein echtes Programm übersetzt wurde. Wie Java kommt auch JavaScript mehr oder weniger ungefragt auf Ihrem Rechner. Implemtierungsfehler sind auch hier nicht ausgeschlossen. Dadurch können die gleichen Sicherheitslücken wie bei Java entstehen.

ActiveX

ActiveX ist von Microsoft als Konkurrenz zu Java entwickelt worden. Logisch, dass es mittlerweile in fast allen Microsoft-Programmen integriert ist. ActiveX sorgt dafür, dass Windows-Anwendungen mit dem Internet zusammenarbeiten. Andere Betriebssysteme sind davon weitgehend ausgeschlossen. Und weil ActiveX sozusagen immer ein Heimspiel hat - denn es wird ja auf einem Windows-System ausgeführt - kann es mit speziellen Funktionen glänzen, die bei Applets nicht so einfach möglich sind. Internetseiten können mit ActiveX um eine Vielzahl von multimedialen Effekten, unterschiedlichen Layouts und ausführbaren Applikationen, die über das Internet geladen werden, erweitert werden.

Die Technologie besteht aus den Elementen: ActiveX-Controls, Active Documents und Active Scripting.

- **ActiveX-Controls** werden auch Steuerelemente genannt und sind Programme, die auf einer Internetseite dargestellt oder als eigene Programme aufgerufen werden können. Die Steuerelemente laufen direkt auf dem Rechner ab und haben Zugriff auf die Hardware und das Betriebssystem.

- **Active Documents** sind dazu da Nicht-HTML-Dokumente (z.B. Word- oder Excel-Dateien) innerhalb eines Browsers anzuzeigen.

- **Active Scripting** verwaltet die ActiveX-Controls und ermöglicht, dass die Steuerelemente miteinander kommunizieren können.

Der **Knackpunkt** von ActiveX ist, dass es **keine richtigen Sicherheitsrichtlinien** gibt. Es gibt zwar signierte ActiveX-Steuerelemente, die versprechen aber nur einen Hauch von Sicherheit. Läuft das ActiveX-Programm erst einmal, dann ist sein Funktionsumfang in keiner Weise eingeschränkt oder kontrollierbar. Das ActiveX-Programm läuft mit allen Rechten des angemeldeten Benutzers - ohne jede Einschränkung! Es ist demnach ein leichtes, private oder sicherheitsrelevante Daten auszulesen, zu löschen, zu manipulieren, den Rechner umzukonfigurieren, einen Virus oder ein Trojanisches Pferd zu installieren.

Cookies

Vielleicht haben Sie folgende Situation schon einmal selbst erlebt: Sie bestellen ab und zu bei einem großen Online-Buchhändler Bücher, CDs oder dergleichen mehr. Immer wenn Sie diese Internetadresse eingeben und sich die Seite aufbaut, werden Sie mit "Hallo Herr xxx!" begrüßt. Aber woher wissen die denn, dass Sie vor dem PC sitzen? Komisch werden Sie sicher denken, der PC hat doch gar keine Augen.

Hat er doch! Und ein Gedächtnis noch dazu. Alles, was ein Web-Server braucht, um Sie als Benutzer beim nächsten Besuch wiederzuerkennen sind Cookies. Eigentlich sind das ja Kekse. Und die krümeln bekanntlich. Diese Krümel sind Informationen - **im Internetumfeld eine kleine Datei, die auf Ihrem PC abgelegt wird**. Natürlich nur, wenn Ihr Browser das will. In dieser Datei werden **Informationen gespeichert**, die im **Zusammenhang mit der jeweiligen Internetseite** stehen. Sie merken das daran, dass Sie beim Ausfüllen des Online-Bestellzettels Daten, die sie einmal eingetragen haben, nicht immer wieder eintippen müssen. Neben der Benutzererkennung werden Cookies auch eingesetzt, um Internetseiten auf Ihre persönlichen Wünsche zuzuschneiden. Die Startseite des Servers kann so nach eigenen Wünschen gestaltet werden, zum Beispiel bei "My Yahoo".

Genau wie Kekse haben auch Cookies eine **bestimmte Lebensdauer**. Manche sind nur so lange aktiv, wie der Browser geöffnet ist, andere haben eine Lebensdauer von mehreren Tagen oder Wochen. Die werden beim Beenden des Browsers dann als Datei in einem "Cookie-Verzeichnis" gespeichert. Wird das "Verfallsdatum" erreicht, werden die Cookies vom Browser automatisch gelöscht. Hat der Browser zu viele Cookies gespeichert, noch bevor die ihr Verfallsdatum erreicht haben - passen also quasi keine neuen Cookies mehr in die Keksdose - dann löscht er die ältesten.

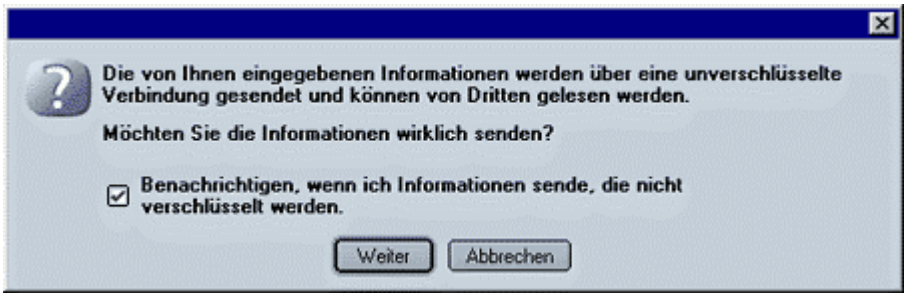
Weil Cookies **keine ausführbaren Programme** sind, stellen sie **kein direktes Sicherheitsrisiko** dar. Es können weder Dateien von der lokalen Festplatte auf den Server, noch Viren übertragen werden. Der Web-Server kann auch nicht auf die Festplatte schreiben. Er kann nur den Browser zum Speichern der Cookies-Datei veranlassen. Nicht unproblematisch ist allerdings die Tatsache, dass durch die Benutzererkennung theoretisch ein sehr genaues Nutzerprofil angelegt werden kann: Surft nur am Wochenende, interessiert sich für klassische Musik etc. Dieses Profil kann für gezielte Werbung genutzt werden. Sie erhalten dann beispielsweise Werbe-E-Mails mit Veranstaltungshinweisen in Ihrer Region - zu klassischer Musik versteht sich.

SSL

Bestimmte Daten sollten beim Internetsurfen (z.B. Kreditkarten-Daten beim Online-Einkauf) verschlüsselt übertragen werden. Ihr Browser bietet Ihnen dazu das Verschlüsselungsverfahren SSL, das eine verschlüsselte Netzverbindung zwischen Server und Browser ermöglicht.

SSL steht für Secure Socket Layer (dt. "sichere Sockelschicht") und wurde von der Firma Netscape und RSA Data Security entwickelt. Das SSL-Protokoll gewährleistet, dass **Daten während der Übertragung nicht gelesen oder manipuliert** werden können und stellt die Identität einer Internetseite sicher. Neben dem Netscape Navigator unterstützt aber auch der Internet Explorer von Microsoft und andere Browser SSL.

Das SSL-Protokoll wird dadurch initiiert, dass dem bekannten http ein s (=secure, dt. sicher) in der URL der Verbindung angehängt wird. Dann lautet die Internetadresse zum Beispiel: https://www.bva.bund.de. Bei jedem Aufruf einer https-Seite, prüft Ihr Browser, ob der Anbieter der Internetseite ein gültiges SSL-Zertifikat hat. Hat er das nicht, dann warnt Sie Ihr Browser mit einer Nachricht: "Diese Web Site kann leider nicht als sicher verifiziert werden. Wollen Sie wirklich weitermachen?"



Bei einer solchen Warnung Ihres Browsers sollten Sie sich in jeden Fall überlegen, ob Sie auf den Seiten dieses Anbieters weitersurfen wollen, da dessen Zertifikat entweder unbekannt oder abgelaufen ist.

Technisch funktioniert SSL wie folgt:

Am "https" erkennt Ihr Browser, dass er vom angesprochenen Server ein Zertifikat anfordern soll. Damit der Server dem Browser ein Zertifikat überhaupt zurückschicken kann, muss er sein Zertifikat von der Zertifizierungsstelle erhalten. Anschließend meldet der Server dieses Zertifikat direkt an den Browser zurück. Der Browser erhält dann vom Verzeichnisdienst der Zertifizierungsstelle die Information, ob das Zertifikat noch gültig ist. Anhand dieser übermittelten Daten kann der Browser nun überprüfen, ob er wirklich mit dem Server verbunden ist, der in der URL angegeben ist. Ist das der Fall, gibt Ihnen Ihr Browser eine entsprechende Information. Beim Internet Explorer erkennen Sie das am geschlossenen Bügelschloss. Der Netscape Navigator/Communicator signalisiert eine sichere Seite durch den intakten Schlüssel.

Anschließend verständigen sich die beiden Rechner auf einen symmetrischen Schlüssel. Diese Verständigung passiert in der sicheren asymmetrischen Verschlüsselung. Um wirklich auf Nummer sicher zu gehen, schickt Ihr Browser dem Server vor dem Beginn des eigentlichen Datenaustausches einige Testnachrichten. Diese kann der Server nur beantworten, wenn es wirklich der Server ist, der er zu sein vorgibt.

Betrachtet man noch einmal die drei Ziele der Verschlüsselung: bewirkt das SSL-Protokoll damit eine sichere Verbindung:

1. Ihre Daten sind **vertraulich**, weil der Inhalt Ihrer Nachrichten nur verschlüsselt über das Netz geht.
2. Die **Authentizität** des Servers steht fest.
3. Ihre Daten sind vor **Manipulation geschützt**, da wirkungsvolle Algorithmen prüfen, ob die Daten vollständig und unverändert ihren jeweiligen Empfänger erreichen.

Als Standard für die Browser-Verschlüsselung hat sich SSL aber bis heute nicht etabliert. Gute Chancen dafür hat das neue Protokoll TLS. Die Abkürzung steht für "Transport Layer Security". Das steht nämlich bereits als potenzieller Nachfolger von SSL in den Startlöchern, weil es noch mehr Sicherheit bei der Kommunikation im Internet verspricht. TLS basiert auf dem noch komplizierteren Verschlüsselungsverfahren Triple-DES (Data Encryption Standard - Datenverschlüsselungs-Standard) oder anderen Algorithmen. Es unterstützt die Verschlüsselung von E-Mails und den Identitätsnachweis für kommerzielle Online-Transaktionen.

Browser-Konfiguration

Das World Wide Web ist bunter und vielfältiger denn je - doch diese Vielfalt hat ihren Preis. Früher war das Risiko beim Betrachten der Internetseiten vergleichsweise gering. Mittlerweile kommen jedoch immer weniger Internetseiten ohne eingebaute Skripte, menügesteuerte Java-Applets oder gar multimedial aufbereitete Präsentationen aus. Diese erweiterte Browser-Funktionen erfordern es, dass unbekannter Code auf Ihrem Rechner ausgeführt wird. Und bekanntlich gefährdet das die Sicherheit Ihres Rechners. Noch dazu ist es bei den Browsern nicht viel anders als bei den normalen Programmen: Sie werden laufend weiterentwickelt, Sicherheitslücken werden geschlossen, neue Lücken tun sich auf ...

Die richtige Browser-Konfiguration

Die **ideale Browsereinstellung für alle Surfer gibt es nicht**. Wenn Sie Ihren Rechner nur zum Spielen benutzen und nebenher ein wenig im Internet surfen, haben Sie niedrigere Ansprüche an dessen Sicherheit als jemand, der darauf wichtige geschäftliche Unterlagen speichert oder Online-Banking betreibt. Und wenn Ihre persönliche Lieblings-Internetseite nur mit Java funktioniert, müssen Sie abwägen, ob Sie zugunsten der Sicherheit ganz darauf verzichten, oder das damit verbundene Risiko in Kauf nehmen wollen.

Die Hersteller stellen die Sicherheitseinstellungen bei der ausgelieferten Browser-Software auf einen **vermuteten Sicherheitsbedarf** ein. Das ist vergleichbar mit

Konfektionsgrößen bei Kleidung - nur, dass es quasi bloß eine gibt. Weil da ja auch nicht jedem alles passt, sollten Sie Ihren Browser also individuell einstellen. So sind Ihnen nicht "die Ärmel zu kurz" und so manche Sicherheitsprobleme lassen sich damit schon vermeiden. Zum anderen sollten Sie regelmäßig auf der Seite des Browser-Herstellers vorbeischauen, ob nicht schon wieder ein Update oder ein Patch für den Browser herausgegeben wurde. Außerdem empfiehlt es sich immer die **neueste Browserversion auf dem PC zu installieren**, weil sich die Hersteller meistens um die Sicherheit der älteren Versionen nicht mehr kümmern. Eigentlich ist das auch kein Problem, schließlich ist die Browsersoftware für Sie kostenlos und kann heruntergeladen werden. Oft liegt sie auch PC-Heften bei. Meistens ist es sogar günstiger, wenn man ein Heft kauft und die Software installiert. Denn das Herunterladen der riesengroßen Browserdateien über ein normales Modem dauert oft viel zu lange und kostet dann genauso viel.

Vor dem Browser-Sicherheits-Check

Durch das Kapitel Datensicherung sind Sie bereits Schritt für Schritt durchgeführt worden. Deshalb sind Ihnen auch Begriffe wie aktivieren, markieren und die Funktionen dahinter bekannt. Die Anleitung zum Sicherheits-Check auf den folgenden Seiten geht deshalb mit weniger Details vonstatten. Sie erfahren dort die wichtigsten Sicherheitseinstellungen für die am häufigsten eingesetzten Browser. Die Einstellungen beziehen sich dabei auf mittlere und hohe Sicherheitsanforderungen.

Und noch ein **letzter Tipp**: Notieren Sie sich Ihre ursprünglichen Einstellungen, bevor Sie etwas verändern. So können Sie - falls doch etwas schief geht - alles wieder in den Originalzustand zurücksetzen.

Der Check beim Internet Explorer 5 und 6

Der erste Schritt

Öffnen Sie im Menü "**Extras**" den Eintrag "**Internetoptionen**".

Aktivieren Sie dann im Fenster "**Internetoptionen**" den Karteireiter "**Sicherheit**".

Wenn Sie es genau wissen wollen: das Zonenkonzept

Der Internet-Explorer arbeitet mit einem so genannten Zonenkonzept, das jeden WWW-Server einer von vier Zonen zuordnet:

1. In die "**Zone Internet**" sind alle Server eingeordnet, die den drei anderen Zonen nicht zuzuordnen sind. Bei Privat-PCs sind das meistens alle.
2. In die "**Zone lokales Intranet**" kommen sowohl die Server eines lokalen Intranets als auch lokale Dateien.
3. Die "**Zone vertrauenswürdige Sites**" ist erst mal leer. Hier können Sie Server eintragen, denen Sie vertrauen, und die deshalb ein wenig mehr auf Ihrem Rechner unternehmen dürfen als andere. Das sind zum Beispiel Server der Online-Shops bei denen Sie häufig einkaufen. Bei denen könnten Sie hinsichtlich aktiver Inhalte eine Ausnahme machen und auch Cookies zulassen.
4. Auch die "**Zone eingeschränkte Sites**" ist zunächst leer. Sie können diese Zone mit Servern füllen, denen Sie misstrauen. Weil Sie grundsätzlich keinem WWW-Server trauen, den Sie nicht kennen, ist die vierte Zone für Privat-Surfer ohne Bedeutung.

Für die einzelnen Zonen können Sie die "Sicherheitseinstellungen" im gleichnamigen Fenster individuell festlegen. Dieses Fenster öffnet sich, nachdem Sie im Fenster "Interneteinstellungen" - siehe oben - auf die Auswahlfläche "Stufe anpassen" geklickt haben.

Benutzerdefinierte Sicherheit - der Maßanzug für Ihren PC

Wie Sie schon durch diesen kleinen Bildausschnitt erkennen können, gibt es eine ganze Menge Sicherheitseinstellungen. Um alle "am Stück" sehen zu können, müssen Sie deshalb jetzt auch ziemlich lange scrollen. Los geht's:

- ActiveX-Steuerelemente und Plugins
  - ActiveX-Steuerelemente ausführen, die für Scripting sicher sind
    - (*) Aktivieren
    - ( ) Deaktivieren
    - ( ) Eingabeaufforderung
  - ActiveX-Steuerelemente initialisieren und ausführen, die nicht sicher sind
    - ( ) Aktivieren
    - ( ) Deaktivieren
    - ( ) Eingabeaufforderung
  - ActiveX-Steuerelemente und Plugins ausführen
    - ( ) Aktivieren
    - ( ) Deaktivieren
    - ( ) Eingabeaufforderung
    - ( ) Vom Administrator genehmigt
  - Download von signierten ActiveX-Steuerelementen
    - ( ) Aktivieren
    - ( ) Deaktivieren
    - ( ) Eingabeaufforderung
  - Download von unsignierten ActiveX-Steuerelementen
    - ( ) Aktivieren
    - ( ) Deaktivieren
    - ( ) Eingabeaufforderung
- Benutzerauthentifizierung
  - Anmeldung
    - ( ) Anonyme Anmeldung
    - ( ) Automatische Anmeldung mit aktuellem Benutzernamen un
    - ( ) Automatisches Anmelden nur in der Intranetzone
    - ( ) Nach Benutzername und Kennwort fragen
- Cookies
  - Cookies annehmen, die gespeichert sind
    - ( ) Aktivieren
    - ( ) Deaktivieren
    - ( ) Eingabeaufforderung
  - Cookies pro Sitzung annehmen (nicht gespeichert)
    - ( ) Aktivieren
    - ( ) Deaktivieren
    - ( ) Eingabeaufforderung
- Download
  - Dateidownload
    - ( ) Aktivieren
    - ( ) Deaktivieren
  - Schriftartdownload
    - ( ) Aktivieren
    - ( ) Deaktivieren
    - ( ) Eingabeaufforderung
- Java
  - Java-Einstellungen
    - ( ) Benutzerdefiniert
    - ( ) Hohe Sicherheit
    - ( ) Java deaktivieren
    - ( ) Mittlere Sicherheit
    - ( ) Niedrige Sicherheit
- Scripting
  - Active Scripting
    - ( ) Aktivieren
    - ( ) Deaktivieren
    - ( ) Eingabeaufforderung
  - Einfügeoperationen über ein Skript zulassen
    - ( ) Aktivieren
    - ( ) Deaktivieren
    - ( ) Eingabeaufforderung
  - Scripting von Java-Applets
    - ( ) Aktivieren
    - ( ) Deaktivieren
    - ( ) Eingabeaufforderung
- Verschiedenes
  - Auf Datenquellen über Domänengrenzen hinweg zugreifen
    - ( ) Aktivieren
    - ( ) Deaktivieren
    - ( ) Eingabeaufforderung
  - Dauerhaftigkeit der Benutzerdaten
    - ( ) Aktivieren
    - ( ) Deaktivieren
  - Installation von Desktopobjekten
    - ( ) Aktivieren
    - ( ) Deaktivieren
    - ( ) Eingabeaufforderung
  - Programme und Dateien in einem IFRAME starten
    - ( ) Aktivieren
    - ( ) Deaktivieren
    - ( ) Eingabeaufforderung
  - Subframes zwischen verschiedenen Domänen bewegen
    - ( ) Aktivieren
    - ( ) Deaktivieren
    - ( ) Eingabeaufforderung
  - Unverschlüsselte Formulardaten übermitteln
    - ( ) Aktivieren
    - ( ) Deaktivieren
    - ( ) Eingabeaufforderung
  - Ziehen und Ablegen oder Kopieren und Einfügen von Dateien
    - ( ) Aktivieren
    - ( ) Deaktivieren
    - ( ) Eingabeaufforderung
  - Zugriffsrechte für Softwarechannel
    - ( ) Hohe Sicherheit
    - ( ) Mittlere Sicherheit
    - ( ) Niedrige Sicherheit

Textversion zur vorangehenden Grafik

Sicherheitseinstellungen

- ActiveX-Steuerelemente und Plugins
  - ActiveX-Steuerelemente ausführen, die für Scripting sicher sind (deaktivieren)
  - ActiveX-Steuerelemente initialisieren und ausführen, die nicht sicher sind (deaktivieren)
  - ActiveX-Steuerelemente und Plugins ausführen (deaktivieren)
  - Download von signierten ActiveX-Steuerelementen (deaktivieren)
  - Download von unsignierten ActiveX-Steuerelementen (deaktivieren)
- Benutzerauthentifizierung
  - Anmeldung (nach Benutzername und Kennwort fragen)
- Cookies
  - Cookies annehmen, die gespeichert sind (deaktivieren)
  - Cookies pro Sitzung annehmen (nicht gespeichert) (Eingabeaufforderung)

- Java
  - Java-Einstellungen (Hohe Sicherheit)
- Scripting
  - Active Scripting (deaktivieren)
  - Einfügeoperationen über ein Script zulassen (deaktivieren)
  - Scripting von Java-Applets (deaktivieren)
- Verschiedenes
  - Auf Datenquellen über Domänengrenzen hinweg zugreifen (deaktivieren)
  - Dauerhaftigkeit der Benutzerdaten (deaktivieren)
  - Installation von Desktopobjekten (deaktivieren)
  - Dateien und Programme in einem IFRAME starten (deaktivieren)
  - Subframes zwischen verschiedenen Domänen bewegen (deaktivieren)
  - Unverschlüsselte Formulardaten übermitteln (Eingabeaufforderung)
  - Ziehen und Ablegen oder Kopieren und Einfügen von Dateien (Eingabeaufforderung)
  - Zugriffsrechte für Softwarechannel (Hohe Sicherheit)

Benutzerdefinierte Sicherheit - der Maßanzug für Ihren PC

Spätestens jetzt schlägt die Stunde des Kompromisses zwischen Ihrem Sicherheitsbedürfnis und Ihrem Bedarf an Komfort beim Surfen. Im Extremfall können Sie gerade Ihre Lieblingsseite nicht sehen, wenn Sie für alle WWW-Seiten die höchste Sicherheit eingestellt haben. Weil dann vielleicht Programme ausgeschlossen sind, die Ihre Seite braucht.

Wenn es Sie nervt, dass beim Surfen dauernd ein Fenster anfragt, ob dieses oder jenes gemacht werden darf, sollten Sie Eingabeaufforderung nur sehr gezielt nutzen. Im Grunde gaukelt diese als Warnung gedachte Einstellung Sicherheit meistens nur vor, weil Sie bei einem unbekannten Server nicht wissen können, ob der angefragten Anwendung zu trauen ist, oder nicht.

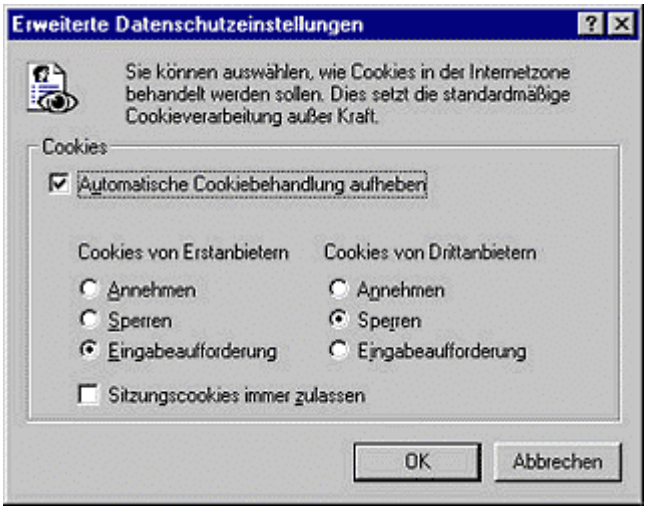
Das muss sein

Bei einigen Anwendungen müssen Sie gar nicht nach dem Komfort fragen - die müssen sein:

- "**ActiveX-Steuerelemente**" deaktivieren.
- "**Download von unsignierten ActiveX-Steuerelementen**" deaktivieren.
- "**Java und JavaScript**" deaktivieren.
  Ausnahme: Bei Web-Servern, deren hohe Sicherheitsstandards Sie kennen - zum Beispiel Homebanking - können Sie sich auf die Kombination "Java, hohe Sicherheit" einlassen.
- "**Active Scripting**" deaktivieren.
- "**Installation von Desktop-Objekten**" deaktivieren.
- "**Zugriffsrechte für Softwarechannel**" auf hohe Sicherheit einstellen.
- "Iframes" und ""Subframes" zwischen verschiedenen Domänen deaktivieren.
- Bei "**Übertragung unverschlüsselte Formulardaten**" Eingabeaufforderung anklicken.

Cookies, Internet Explorer 6

Wie im richtigen Leben sind Cookies Geschmacksache.
Unter "**Internetoptionen**" - Karteireiter "**Datenschutz**" - Auswahl "**erweitert**" können Sie die Einstellungen ändern:



Wenn Sie vor "**Automatische Cookiebehandlung aufheben**" durch einen Klick das Häkchen setzen, lässt sich eine individuelle Lösung festlegen, zum Beispiel diese:

- **Cookies von Drittanbietern sperren**. Das sollten Sie auf jeden Fall tun, weil sie meistens nur der Nutzerprofilerstellung dienen.

- Falls Sie Cookies von **Erstanbietern**, also von Servern, die Sie besuchen, **nicht deaktivieren** möchten, aktivieren Sie **Eingabeaufforderung**.

- **Sitzungscookies** sind Cookies, die während **einer Surf-Aktion** entstanden sind. Beim Verlassen des Internet Explorers werden sie gelöscht. Wenn Sie nur wenige Server anwählen und diesen die Verwendung von Cookies erlauben möchten, können Sie diese Server unter "Bearbeiten" einzeln eintragen und festlegen "annehmen" oder "ablehnen".

Cookies, Internet Explorer 5

Für den IE 5 finden Sie die Einstellungen "Cookies" unter den allgemeinen Sicherheitseinstellungen. Dort gibt es nur die Unterscheidung zwischen Sitzungscookies und anderen Cookies. Das sollten Sie **deaktivieren**. Falls Sie möchten, dass einzelne Server Cookies akzeptieren sollen, können Sie die Eingabeaufforderung einschalten.

Erweiterte Einstellungen

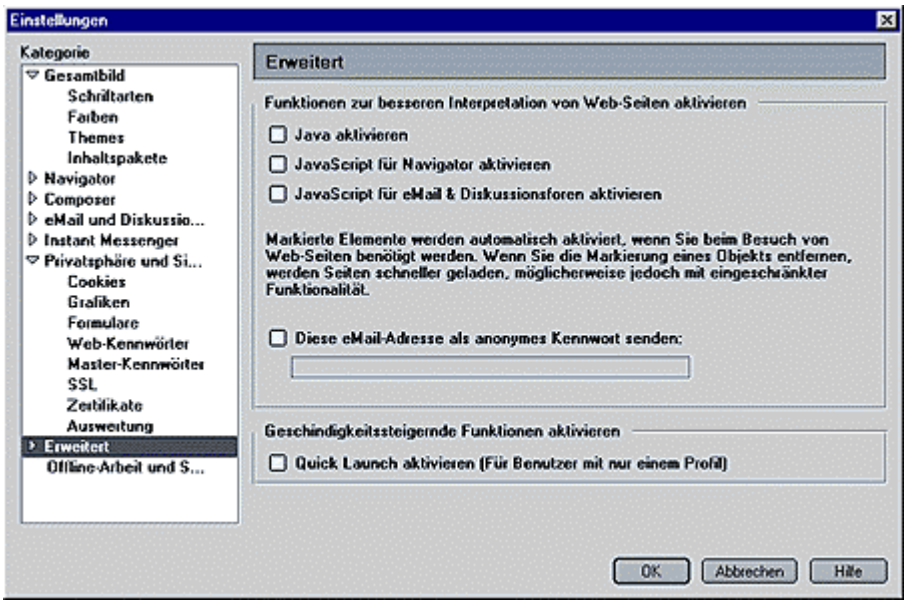
Unter dem Karteireiter "Erweitert" deaktivieren Sie das "automatische Update". Dadurch könnte Ihnen nämlich jemand eine manipulierte Version unterschieben. Öffnen Sie das automatische Update nur bei Bedarf, und auch nur dann, wenn nur ein Fenster geöffnet ist, in dem die Microsoft-Webseite geladen ist.

Aus gleichem Grund deaktivieren Sie "Installation bei Bedarf". Dabei geht es nämlich keineswegs um Ihren Bedarf: Dort werden automatisch Komponenten des Browsers oder Zusatzprogramme geladen, wenn sie für die Darstellung bestimmter Inhalte gebraucht werden.

Der Check bei Netscape 6.x und Mozilla

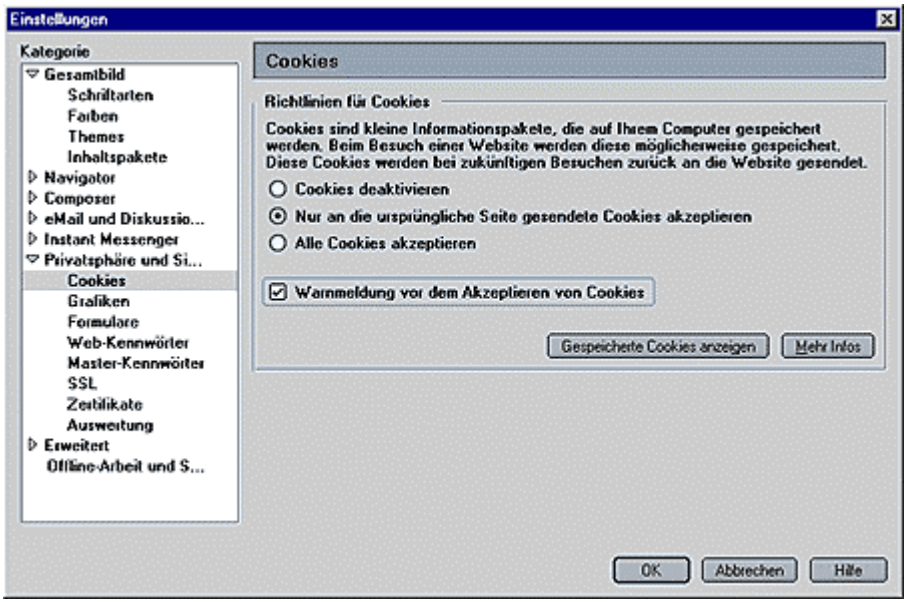
Weil Netscape 6.* im Wesentlichen auf Mozilla basiert, sind die Einstellungen für die Sicherheit bei beiden gleich.

Java und JavaScript



Unter **Erweitert** müssen Sie "**Java und JavaScript deaktivieren**". Weil Sie manchmal - zum Beispiel beim Online Banking - JavaScript wieder einschalten müssen, dürfen Sie nicht vergessen, "**JavaScript bei Mail und News**" zu "deaktivieren". Denn Mail und News benötigen praktisch nie JavaScript, weshalb sie mit einer sicheren Einstellung abgerufen werden sollen.

Cookies



Unter "**Privatsphäre**" und "**Sicherheit**" können Cookies deaktiviert werden. Wenn Sie das nicht wollen, schalten Sie **auf jeden Fall die Warnmeldung vor dem Akzeptieren von Cookies ein**.

Weitere Sicherheitseinstellungen

Unter "**Erweitert - Software Installation**" **deaktivieren Sie die automatische Software-Installation**. Die Gründe dafür finden Sie beim Microsoft Explorer oben.

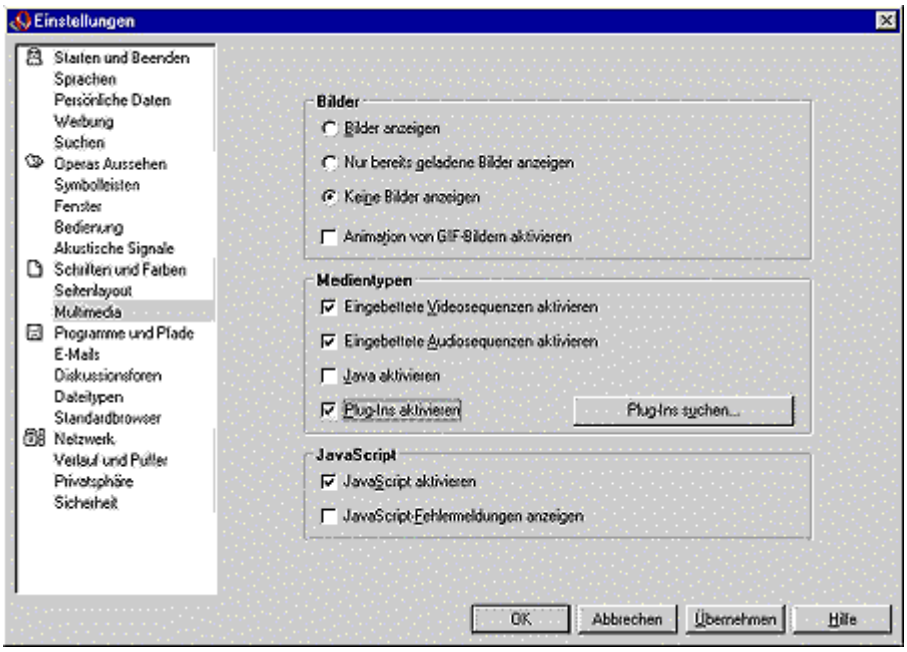
Die Einstellungen für den "**PGP-verschlüsselten Zugriff auf WWW-Server**" finden Sie unter "**Erweitert - SSL**". Hier **deaktivieren Sie das Senden von Formulardaten von einer unsicheren Seite zur anderen**. Deaktivieren Sie das nicht, können vertrauliche Daten ausspioniert werden.

Der Check bei Opera 5 und 6

Alle Einstellungen erreichen Sie über das Menü "**Datei**" und "**Einstellungen**".

Java und JavaScript

JavaScript und Java lassen sich bei Opera 5 unter PlugIns deaktivieren. Bei Opera 6 finden Sie die entsprechende Einstellung unter "**Multimedia**". Die Einstellungen gelten global, denn Opera arbeitet nicht mit einem Zonenmodell, wie der Microsoft Explorer.

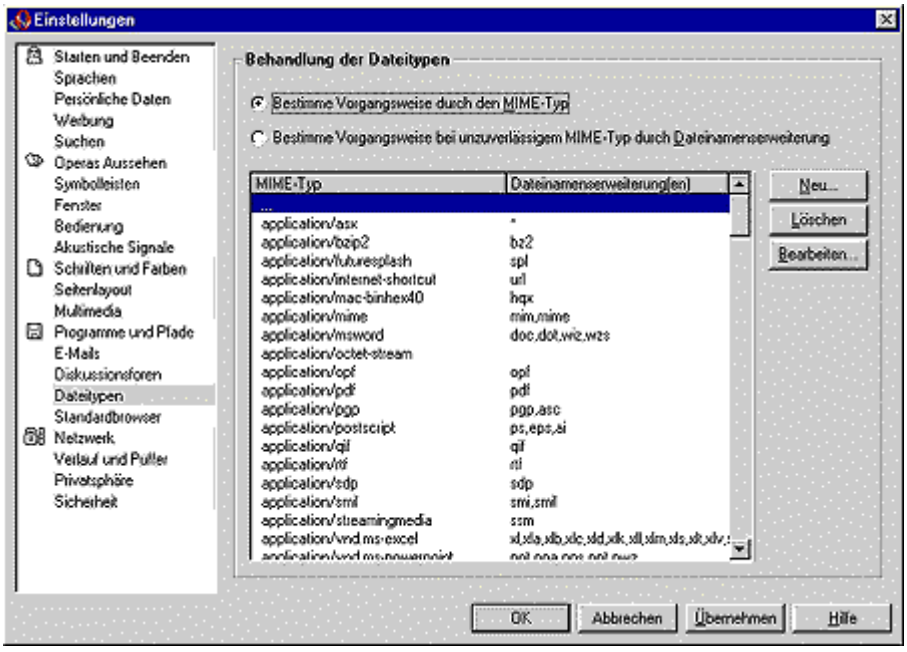


Persönliche Einstellungen

Im Fenster "**Einstellungen**" können Sie persönliche Daten wie Namen und Adresse hinterlegen. Die können dann automatisiert in Web-Formulare übertragen werden. Ganz Vorsichtige hinterlegen allerdings nichts. Was nicht drin steht, kann auch nicht versehentlich übertragen werden. Eine Sicherheitslücke, die das Auslesen dieser Daten ermöglicht, ist derzeit allerdings nicht bekannt.

Dateitypen

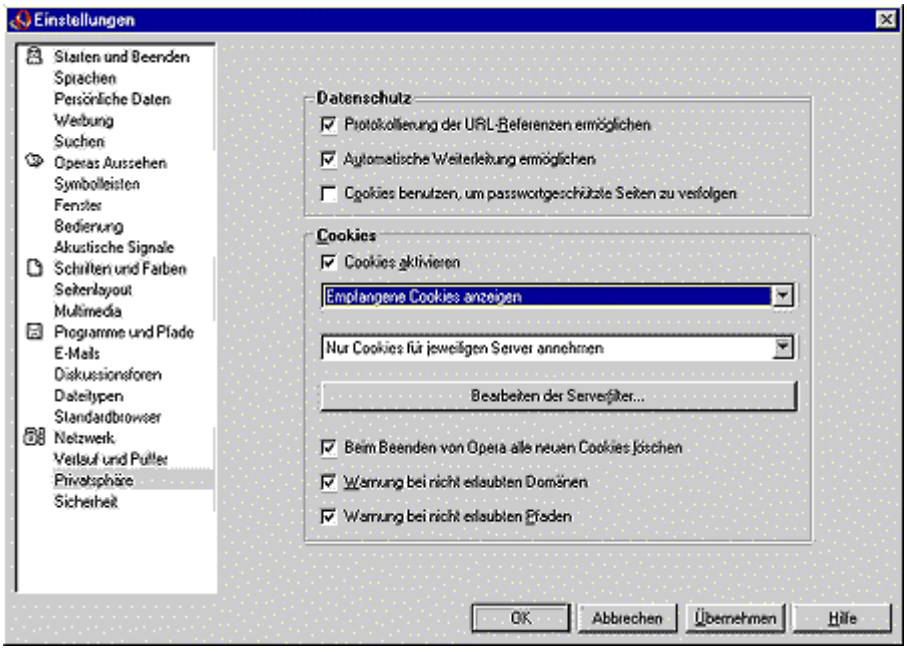
Unter "**Dateitypen**" stellen Sie ein, wie Opera verschiedene Dateien behandelt, die nicht direkt angezeigt werden können. Sie sollten dort aktivieren: Aktion durch MIME-Typ festlegen, falls glaubwürdig. Damit erreichen Sie, dass nicht nur aus der Datei-Endung auf den Dateityp geschlossen wird. Das wäre nämlich mit zusätzlichen Missbrauchsmöglichkeiten verbunden.



Wie Opera mit jedem einzelnen Dateityp umgehen soll, können sie durch Auswahl und Bearbeiten einstellen. Problematisch in punkto Sicherheit sind makrofähige Dateiformate, beispielsweise das Microsoft Word Format doc. Hierfür - und auch für andere Microsoft-Office-Formate - finden Sie auf Microsofts WWW-Seiten ein Programm namens wordviewer (bzw. excelviewer etc.). Der versteht das Format, kann aber keine Makros ausführen. Opera kann mit dem Wordviewer arbeiten - und Windows darf trotzdem andere Programme nutzen.
Wenn Sie den Wordviewer nicht wollen, gibt es eine Alternative. Sie können Auswahl und Bearbeiten auch so einstellen, dass derartige Dateien nicht geöffnet, sondern nur herunter geladen werden sollen. Dann können Sie die Datei vor dem Öffnen von einem Virenscanner kontrollieren lassen.
Die Voreinstellung "Zeige Download-Dialog" ist nützlich und sollte nicht geändert werden.

Cookies

In "**Privatsphäre**" geht es um die Cookies. Wenn Sie Cookies nicht grundsätzlich abschalten möchten, lassen Sie sich alle empfangenen Cookies anzeigen. Angenommen werden aber nur Cookies von dem Server, den Sie gerade besuchen.



In "**Bearbeiten der Server-Filter**" deaktivieren Sie die Möglichkeit "**Cookies benutzen, um passwortgeschützte Dokumente zu verfolgen**". Bleibt diese Einstellung aktiv, kann sich jemand - zum Beispiel mit einem Trojanischen Pferd - bei Ihnen ein Cookie holen und dann auf geschützte Seiten, auf die eigentlich nur Sie Zugriff haben sollten, zugreifen.

Noch ein Tipp: Unter "**Datei**" und dann "**Private Informationen löschen**" können mit einem einzigen Mausklick alle persönlichen Informationen wie Verlauf, History, Cookies oder Cache gelöscht werden.

Werbung im Internet

Da die meisten Anbieter ihre **Internetinhalte für Sie kostenfrei** zur Verfügung stellen, stellt sich die Frage, wie diese ihre Internetseite überhaupt finanzieren. Schließlich beansprucht die Pflege der Inhalte Zeit und Geld. Werbung im Internet in allen erdenklichen Formen ist hier das Schlüsselwort. Es gibt kaum eine Seite auf der man keine sieht. Überall blinkt und zappelt es. Das kann beim Surfen ziemlich schnell lästig werden. Schlimm genug, dass man ständig irgendwelche Werbefenster schließen muss, das Laden der Seite dauert oft auch noch ziemlich lange. Die Zeit, die Sie warten, bedeutet für Ihren Provider Geld. Schließlich zahlen Sie ja nach Minuten, wenn Sie keine Flatrate haben.

Wenn Sie die Werbung im Internet dauerhaft unterdrücken wollen, müssen Sie einen Content-Filter installieren. Diese Software sorgt dafür, dass Ihr Browser nur die Inhalte und nicht die Werbung der Internetseite darstellt. Ein solches Programm finden Sie übrigens auch in unserer Toolbox.

Quelle: http://www.bsi-fuer-buerger.de/03/

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**.

So arbeitet Ihr PC

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.

So gehen Daten verloren

Manchmal löscht man selbst Daten versehentlich. Bei modernen Betriebssystemen gibt es deshalb eine Art **Papierkorb**. Dorthin gelangen die gelöschten Dateien erst einmal. Wenn Sie nun merken, dass Sie die Datei ja doch noch brauchen, können Sie die Datei jederzeit wieder herstellen. Haben Sie den Papierkorb jedoch geleert, dann sind die darin enthaltenen Dateien endgültig gelöscht.

Eine Datei kann auch für immer und ewig verloren gehen, wenn Sie diese überschreiben. Meistens passiert das, wenn Sie ein bereits bestehendes Textdokument öffnen, um es als Vorlage für ein neues Schreiben zu benutzen. Wenn Sie das Dokument dann ändern und versehentlich auf "speichern" klicken, wird die eigentlich neue Datei unter dem alten Dateinamen abgespeichert und der Inhalt des alten Dokuments ist futsch.

Und schließlich können Daten auch verloren gehen, wenn Sie den PC nicht vorschriftsgemäß herunterfahren, sondern einfach ausschalten. Möglicherweise entstehen dabei nämlich Inkonsistenzen im Dateisystem. Die führen dazu, dass Sie Dateien, die auf dem Rechner gespeichert sind, nicht mehr wiederfinden.

Logisch ist natürlich auch, dass alle Daten weg sind, wenn Ihr PC gestohlen wird. Laptops sind dabei besonders beliebte Objekte.

Diese Daten sollten Sie sichern

Aber genug der Schwarzmalerei, schließlich gibt es für alle diese Probleme eine Lösung: die Datensicherung. Dabei werden alle Daten, die Sie brauchen - im Zweifelsfall also alle - regelmäßig auf einen Datenträger kopiert, den Sie anschließend sicher verwahren können.

Welche Dateien sollen ausgelagert werden?

Betriebssystem und Programme:

Werden Dateien des Betriebssystems und der installierten Programme beschädigt, kann das dazu führen, dass ein Anwendungsprogramm oder auch das Betriebssystem nicht mehr funktioniert. Trotzdem müssen diese Dateien **nicht zwingend gesichert** werden. Denn meistens gibt es fürs Betriebssystem Reperaturmechanismen. Oder man installiert das Betriebssystem mit den Original-CDs neu. Auch Anwendungsprogramme, zum Beispiel die Textverarbeitung, können jederzeit vollständig deinstalliert und von den Original-CD-ROMs wieder hergestellt werden. Eine Ausnahme gibt es allerdings: Wenn Sie die Programme auf Ihre Bedürfnisse hin verändert haben, dann sollten Sie die so genannten Konfigurationsdateien extern speichern, weil Ihre Änderungen darin abgespeichert sind. Dazu zählen auch Wörterbücher. Das sind Dateien, in die Sie Wörter geschrieben haben, die Ihr PC bei der Rechtschreibprüfung noch nicht kannte. Achtung: Ihre Anwendungsprogramme, Konfigurationsdateien, Wörterbücher etc. verschwinden, wenn Sie das Betriebssystem komplett neu aufspielen. Sichern Sie also alle wichtigen Dateien vorher!

Anwendungsdaten:

Viel schlimmer ist der Verlust der Anwendungsdaten, also Dateien, die Sie selbst erstellt und auf dem Computer gespeichert haben. Das können Texte, Bilder, Tabellen oder andere Dokumente sein. Verschwinden diese Informationen, sind sie auf Nimmerwiedersehen verloren. Da hilft kein Zaubern, sondern nur eine regelmäßige Datensicherung.

Wie viel Aufwand Sie bei der Datensicherung betreiben, also wie oft Sie welche Dateien extern abspeichern, hängt ganz allein von Ihnen ab. Und davon, wie viel Zeit Sie fürs Speichern und Suchen investieren wollen.

Methoden der Datensicherung:
Wie wird gespeichert?

Volldatensicherung

Bei der Volldatensicherung werden sämtliche zu sichernden Dateien zu einem bestimmten Zeitpunkt auf einen zusätzlichen Datenträger gespeichert.

Vorteil: Alle Daten liegen komplett vor. Sie müssen bei der Wiederherstellung der Dateien nicht lange suchen.

Nachteil: Je nachdem, wie viele Daten Sie speichern, kann die Volldatensicherung sehr zeitaufwendig sein und viel Platz auf dem Speichermedium verbrauchen.

Inkrementelle Datensicherung

Dazu müssen Sie einmal eine Volldatensicherung durchführen. Danach werden nur noch die Dateien gesichert, die sich seit der letzten Volldatensicherung bzw. seit der letzten inkrementellen Datensicherung verändert haben.

Vorteil: Sie sparen Speicherplatz und brauchen weniger Zeit für die Datensicherung.

Nachteil: Was Sie an Zeit bei der Datensicherung sparen, müssen Sie im Zweifelsfall bei der Wiederherstellung der Daten einplanen. Denn im Bedarfsfall müssen Sie zunächst die letzte Volldatensicherung auf das System übertragen. Anschließend müssen alle nach der Volldatensicherung angefertigten inkrementellen Datensicherungen eingespielt werden. Auch wenn nur eine einzelne Datei wiederhergestellt werden soll, ist der Aufwand gegenüber der Volldatensicherung höher, da Sie alle inkrementellen Datensicherungen und vielleicht sogar die letzte Volldatensicherung durchsehen müssen, um die aktuelle Version einer Datei zu finden.

Differentielle Datensicherung

Auch dazu müssen Sie einmal eine Volldatensicherung durchführen. Danach werden bei jeder differentiellen Datensicherung alle Daten gesichert, die sich seit der letzten Volldatensicherung verändert haben.

Vorteil: Die Wiederherstellung der Dateien ist im Bedarfsfall unkomplizierter und schneller. Sie müssen dann nur die letzte Volldatensicherung und die aktuelle differentielle Datensicherung parat haben.

Nachteil: Gegenüber der inkrementellen Datensicherung brauchen Sie mehr Zeit und Platz auf dem Speichermedium.

Die Technik: Worauf wird gespeichert?

Für welche Datensicherungsstrategie Sie sich entscheiden, hängt zum einen davon ab, wie groß die Datenmenge ist, die Sie sichern wollen und ob Sie viel an den jeweiligen Programmeinstellungen geändert haben. Zum anderen ist natürlich auch die Kapazität der externen Speichermedien entscheidend.

- Speichermedien
Als Speichermedien bieten sich für private Zwecke Diskettenlaufwerke, ZIP-Laufwerke, CD-ROM-Brenner oder Wechselfestplatten an. Auch Bandlaufwerke sind sehr geeignet - im Zweifelsfall für den Privatgebrauch aber zu teuer. Normale Diskettenlaufwerke eignen sich aufgrund der geringen Speicherkapazität von Disketten eher nur bei geringer Datensicherungsmenge. Wenn Sie mehr sichern wollen, nehmen Sie ZIP-Laufwerke, CD-ROM-/DVD-Brenner und Wechselfestplatten.

- Software
Wenn Sie Ihre Datensicherung automatisieren wollen, brauchen Sie zusätzliche Software. Im Lieferumfang einiger Betriebssysteme, wie z. B. Windows 95/98/2000 und XP oder einer der verschiedenen Linux-Distributoren, befindet sich ein Datensicherungstool, das Sie auch ohne Bandlaufwerk einsetzen können. Daneben gibt es auch eine Reihe von Free- und Shareware-Produkten.

So organisiert man die Datensicherung

Wie Sie bei der Datensicherung vorgehen können, zeigt folgendes Beispiel:

Angenommen,
... Sie nutzen Ihren Computer nur privat und benutzen ihn nicht täglich.

... Ihr Gesamtbestand an Dateien mit Anwendungsdaten (z. B. Textdateien) ist so groß, dass eine Speicherung auf Disketten nicht in Frage kommt.

... die Dateien, die Sie selbst während einer Arbeitssitzung erstellt oder verändert haben, lassen sich hingegen auf einer Diskette speichern. Der Rechner verfügt über einen CD-ROM-Brenner.

In diesem Fall entschließen Sie sich nach dem Abwägen der Vor- und Nachteile der verschiedenen Methoden für die **inkrementelle Datensicherung**. Dazu benötigen Sie **drei wiederbeschreibbare CD-ROMs**, die Sie mit den Ziffern 1 bis 3 **durchnummerieren**, und **fünf ebenfalls nummerierte Disketten**.

Dann gehen Sie wie folgt vor:

Zunächst führen Sie eine **Volldatensicherung** durch. Weil die Datensicherungssoftware bei Ihnen vermutlich kein Bandlaufwerk findet, legt sie auf der Festplatte des Rechners eine Datei an, in die die zu sichernden Daten abgespeichert werden. Diese Daten brennen Sie nach Abschluss der Datensicherung auf die CD-ROM Nr. 1.

An Tagen, an denen Sie Dateien erstellt oder verändert haben, führen Sie am Ende der Rechnerbenutzung eine **inkrementelle Datensicherung** durch. Die erste inkrementelle Datensicherung wird auf der Diskette Nr. 1 abgespeichert, die zweite auf der Diskette Nr. 2 usw. Wenn sich nun auf allen fünf Disketten inkrementelle Datensicherungen befinden, machen Sie nach der nächsten PC-Benutzung eine neue Volldatensicherung auf der CD-ROM Nr. 2. Danach kann der Inhalt der fünf Disketten gelöscht werden. Diese können Sie dann wieder zu inkrementellen Datensicherungen einsetzen. Wenn die fünf wieder voll sind, ist die nächste Datensicherung wieder eine Volldatensicherung auf der CD-ROM Nr. 3. Dieses Spiel geht jetzt immer so weiter. Sie können jetzt entweder bei der nächsten Volldatensicherung die CD-ROM Nr. 1 überschreiben (natürlich nur, sofern Sie eine wiederbeschreibbare CD-ROM verwendet haben) oder Sie heben diese auf und nehmen neue CD-ROMs. Auf die Fragen, wie lange man Volldatensicherungen aufbewahren sollte, gibt es allerdings keine pauschale Antwort. Wenn Sie zum Beispiel gerade an Ihrer Diplomarbeit, Steuererklärung oder ähnlichem sitzen, sollten Sie alle Datensicherungen aufheben - zumindest so lang wie Sie die Daten unbedingt benötigen. Außerdem gibt es Dateien, die nur selten gebraucht werden. Sofern solche Dateien auf der Festplatte beschädigt werden, fällt dies häufig erst so spät auf, dass nur eine ältere Datensicherung eine Wiederherstellung erlauben würde.

Nach jedem Datensicherungslauf sollten Sie prüfen, ob Sie auch alle für die Datensicherung festgelegten Dateien gespeichert haben. Dazu hat verfügt die Datensicherungs-Software meistens über eine entsprechende Überprüfungsfunktion. Sofern die Datensicherungs-Software zusätzlich Protokolle erzeugt, sollten diese auf jeden Fall regelmäßig durchgesehen werden.

Beispiele für die Datensicherung

Das Betriebssystem Windows bietet Ihnen die Möglichkeit Daten über das Datensicherungsprogramm zu sichern und im Falle eines Datenverlustes auch wiederherzustellen. Nach dem Aufrufen des Datensicherungsprogramms werden Sie Schritt für Schritt angeleitet. Auf den folgenden Seiten finden Sie das für Windows 98 und Windows XP anhand eines einfachen Beispiels demonstriert:

Windows 98

- Volldatensicherung Windows 98
- Inkrementelle Datensicherung Windows 98
- Wiederherstellung von Daten Windows 98

Windows XP

- Volldatensicherung Windows XP
- Inkrementelle Datensicherung Windows XP
- Wiederherstellung von Daten Windows XP

Leider gibt es bei diesem Programm keine integrierte Hilfefunktion. Tauchen Probleme auf, bei denen Sie nicht weiter wissen, wenden Sie sich bitte direkt an den Hersteller Ihres Betriebssystems.

Wenn Sie Produkte der Firma Microsoft verwenden - wie bei den dargestellten Beispielen - können Sie sich an die **Microsoft Telefonhotline** unter der Nummer 0180 5 67 22 55 (Euro 0,12/min) wenden. Weitere Informationen erhalten Sie auch auf der dieser Internetseite: Microsoft-Support

Wenn Ihnen das alles zu kompliziert ist und Sie über ein ZIP-Laufwerk oder einen CD-ROM oder DVD-Brenner verfügen, dann gibt es auch eine andere Möglichkeit: Speichern Sie Ihre Anwendungsdaten - also Dateien, die Sie selbst erstellt haben - auf einem externen Speichermedium. Wie oft das notwendig ist, hängt davon ab, wie oft Sie Ihren PC nutzen und welche Daten Sie in jedem Fall benötigen. **Bewahren Sie das Backup aber auf jeden Fall getrennt vom PC auf**, am besten in einem anderen Raum. Sollten Sie Ihre Daten später aus irgend einem Grund verlieren, können Sie Ihre Anwendungsdaten einfach wieder auf den PC aufspielen. Ihre persönlichen Einstellungen des Betriebssystems oder anderer Programme sind bei dieser Art der Datensicherung zwar nicht enthalten, aber diese lassen sich im Falle des Falles wiederherstellen. Alternativ zu CD-ROM, DVD oder ZIP-Laufwerken können Sie auch eine zweite Festplatte als Datensicherungsmedium verwenden. Damit diese nach der Datensicherung an einem anderen - sicheren - Ort aufbewahrt werden kann, sollte es eine Wechselfestplatte sein.

Sie haben also die Wahl: Entweder Sie nutzen **ein Datensicherungstool** oder Sie speichern nur Ihre Anwenderdaten regelmäßig auf einem **externen Speichermedium**. Für den Fall, dass Sie sich nicht zwischen den beiden Möglichkeiten entscheiden können, gilt: Doppelt hält besser!

Die letzte Rettung

Sollten Ihre versehentlich gelöschten oder "korrupt" (beschädigt) gewordenen Daten nicht mit dem Datensicherungsprogramm wiederherstellbar sein, können sogenannte "Datenretter" im wahrsten Sinne des Wortes Ihre letzte Rettung sein. **Verschiedene Softwarehersteller bieten dazu Programme an**. Wenn Sie selbst damit nichts retten können, gibt es Firmen, die Daten im Speziallabor retten können. Weil das allerdings ziemlich teuer werden kann, sollten Sie vorher klären, ob sich der Aufwand lohnt.

Quelle: http://www.bsi-fuer-buerger.de/03/03080701.htm

Datensicherung bei Linux

1. Welche Daten sollten Sie sichern?

Wenn Sie das Betriebssystem Linux verwenden, dann gibt es - wie bei anderen Betriebssystemen auch - mehrere Möglichkeiten Ihre Daten zu sichern. Die sicherste Backup-Strategie ist das **Duplizieren der Festplatte.**
Hierzu kann man mit dem UNIX-Befehl **dd** ein physikalisches Abbild der ersten Festplatte auf eine zweite Festplatte oder ein Image auf Band übertragen.
Beispiel:
IDE-Festplatte 1 wird auf IDE-Festplatte zwei gespiegelt
`dd if=/dev/hda of=/dev/hdb bs=128k`

IDE-Festplatte 1 wird auf den ersten SCSI-Streamer gesichert
`dd if=/dev/hda of=/dev/st0 bs=512`
Möchte Sie aus Zeit und/oder Platzgründen nicht die gesamte Platte sichern, sollten Sie zumindest die wichtigsten Verzeichnisse speichern:

- das **home**-Verzeichniss (beinhaltet die Anwendungsdaten der einzelnen User)
- das **root**-Verzeichnis
- die Konfigurations-Verzeichnisse **etc** und **var**.

Die restlichen Verzeichnisse können meist durch das Aufspielen des Betriebssystems und der Anwendungsprogramme wiederhergestellt werden. Vergessen Sie dabei nicht, auch die eingespielten (Sicherheits-) Patches zu sichern (z.B. die Patches unter **/home/patch/**Versionxxx ablegen).

2. Welche Software gibt es?

Als Datensicherungssoftware wird meistens das Programm **tar** eingesetzt. Diese Software kann sehr flexibel über die Komandozeile konfiguriert werden und ist vom Backup-Medium unabhängig.
Beispiel:
Ein einfaches Backup erzeugt man auf der Kommandozeile aus dem Verzeichnis **/** :
`tar -czvf /BACKUPdir/NAME.tgz /home /etc /var` erzeugt eine Backup-Datei
`tar -czvf /dev/st0 /home /etc /var` erzeugt ein Backup auf Band
Um das Backup zu **Verifizieren** dienen folgende Kommandozeilen aus dem Verzeichnis / :
`tar -dzvf /BACKUPdir/NAME.tgz /home /etc /var`
`tar -dzvf /dev/st0 /home /etc /var`

Zum **Rücksichern** gibt man folgende Kommandozeile aus dem Verzeichnis **/** ein:
`tar -xzvf /BACKUPdir/NAME.tgz`
`tar -xzvf /dev/st0`

Möchten Sie nur **bestimmte** Dateien **wiederherstellen**, können Sie diese auch mit ihrem Verzeichnis-Namen als Parameter mit angeben.

Beispiel:
/etc/passwd oder /home/NAME/mailbox
(Siehe auch unter den Man-Pages oder tar --help.)
Fertige Shell-Scripte dazu finden Sie übrigens auf www.linux-backup.net.
Ein weiteres **Kommandozeilen-Tool** ist das Programm **cpio**. Wenn Sie statt einem Kommandozeilen-Tool ein Programm mit **grafisches Frontend** benutzen wollen, so bietet sich **KBACKUP** oder unter der KDE Oberfläche das Programm **KDAT** für SCSI und Tape-Streamer an.

Quelle: http://www.bsi-fuer-buerger.de/03/03080101.htm

Volldatensicherung bei Windows 98

Wenn das Programm dort nicht verfügbar ist, müssen Sie es installieren. Dazu gehen Sie im Startmenü auf den Menüpunkt "Einstellungen" und dort auf "Systemsteuerung". Es öffnet sich ein Fenster. Darin das Verzeichnis "Software" anklicken:

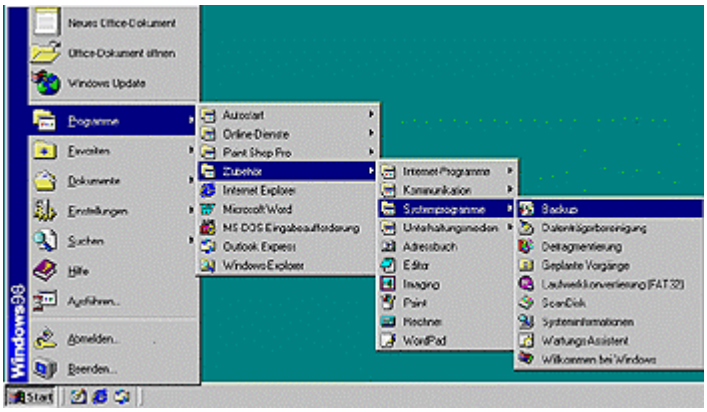
Im Fenster, das sich danach öffnet, wählen Sie bitte die Registerkarte "Windows Setup" aus. In der nächsten Ansicht klicken Sie auf den Menüpunkt "Systemprogramme".

Im nun folgenden Fenster klicken Sie ins Kästchen vor der Komponente "Backup". Wenn es richtig ist, fügt sich dort ein Häkchen ein.

Danach bestätigen Sie Ihre Auswahl durch Klick auf die Schaltfläche "OK".
Jetzt erscheint ein weiteres Fenster. Auch hier klicken Sie bitte die Schaltfläche "OK" an. Danach wird das Datensicherungsprogramm installiert. Anschließend müssen Sie den Rechner neu starten.

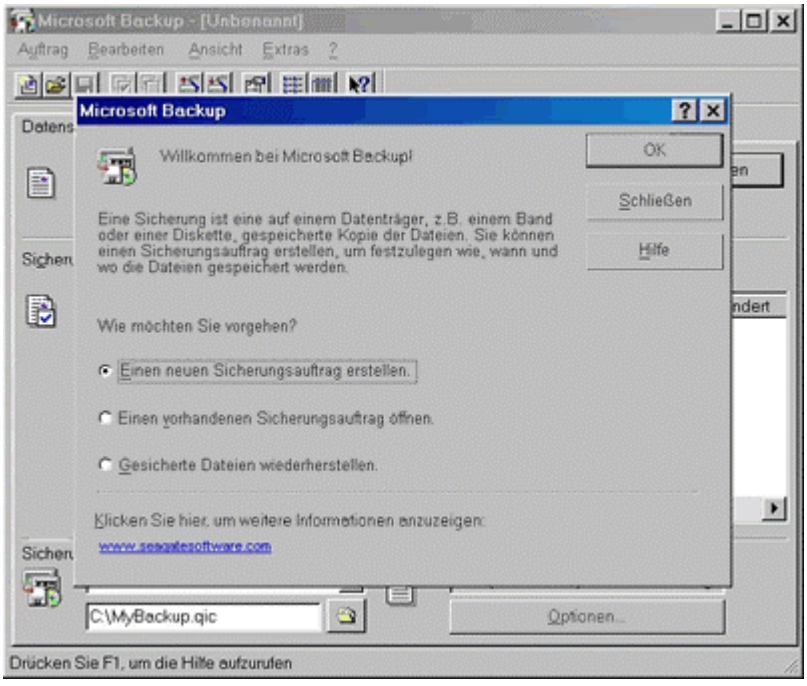
Zum Start des Datensicherungsprogramms wählen Sie bitte im **Startmenü** den Menüpunkt "**Programme**" und in dem sich öffnenden Fenster das Verzeichnis "**Zubehör**" aus. Es öffnet sich erneut ein Fenster, in dem Sie das Verzeichnis

"**Systemprogramme**" auswählen. Im nächsten Fenster starten Sie das Programm "**Backup**" durch einen Klick mit der Maus.



Wenn Sie das Programm zum ersten Mal starten, öffnet sich ein Fenster mit folgender Meldung:

Wenn Ihr Rechner **kein Bandlaufwerk** hat, müssen Sie die Schaltfläche "**Nein**" anklicken. Danach öffnet sich ein Fenster.



Hier haben Sie die Möglichkeit anzugeben, ob ein neuer Datensicherungsauftrag erstellt, ein vorhandener Datensicherungsauftrag geöffnet oder gesicherte Dateien wiederhergestellt werden sollen. Weil das Programm jetzt das erste Mal benutzt wird,

müssen Sie den Punkt "Einen neuen Sicherungsauftrag erstellen" auswählen. Da dies die Standardeinstellung ist, genügt die Bestätigung per Mausklick auf die Schaltfläche "OK".

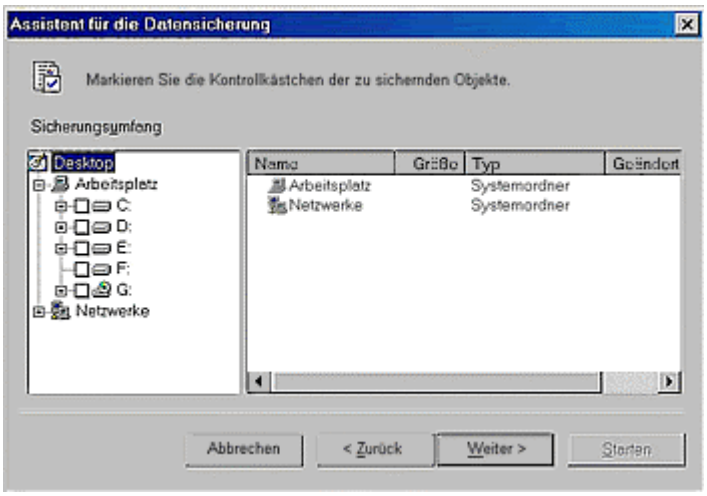
Hier noch ein Hinweis: Den zweiten Auswahlpunkt brauchen Sie, wenn Sie schon einmal Datensicherungen gemacht haben, und die neue genau so durchgeführt werden soll. Der dritte Auswahlpunkt erklärt sich selbst.

Es öffnet sich ein Fenster mit dem Datensicherungs-Assistenten.

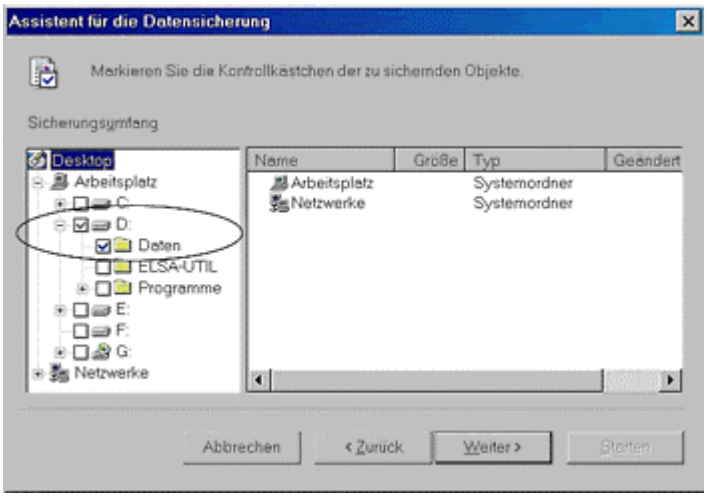
Da im Beispiel beabsichtigt ist, lediglich die Dateien mit den Anwendungsdaten, die sich in dem Verzeichnis D:\Daten (es können bei Ihnen natürlich auch andere sein) und in den darunter liegenden Verzeichnissen befinden, zu sichern, wählen Sie bitte die zweite Möglichkeit ("Markierte Dateien") aus.

Mit der ersten Auswahlmöglichkeit ("Arbeitsplatz" sichern) können Sie eine Komplettsicherung des gesamten Rechners, das heißt aller auf den lokalen Laufwerken gespeicherten Dateien durchführen. Das wollen Sie jetzt aber nicht.

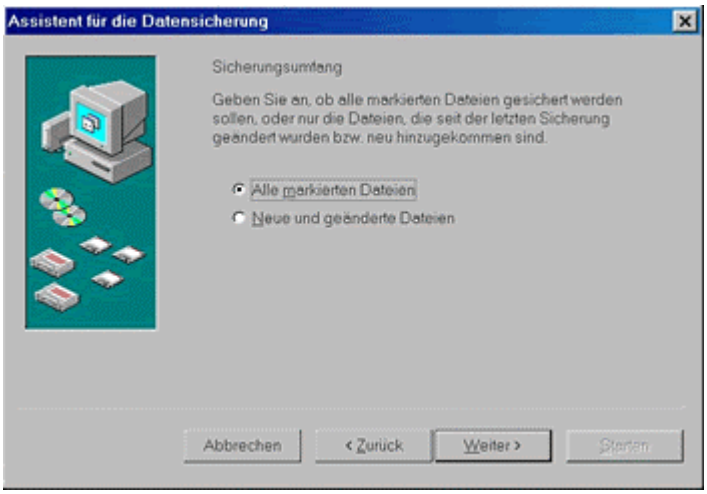
Nun klicken Sie auf die Schaltfläche "Weiter " Sie sehen dann dieses Fenster:



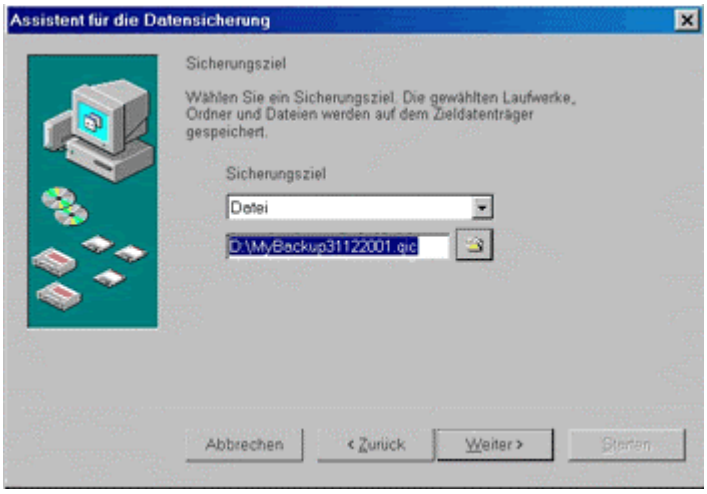
Dort können Sie nun die Laufwerke oder auch nur einzelne Verzeichnisse oder Dateien zur Datensicherung auswählen. Dazu klicken Sie einfach mit der Maus in das entsprechende Kästchen. Wenn auf diese Weise in das leere Kästchen beispielsweise vor dem Laufwerk D: geklickt wird, werden für die Datensicherung alle darunter befindlichen Verzeichnisse und Dateien ausgewählt. Wird auf das Kästchen mit dem "+"-Zeichen geklickt, öffnet sich der Verzeichnisbaum mit weiteren Auswahlkästchen. Als Beispiel soll dies nun für das Verzeichnis "Daten" auf dem Laufwerk D: für die Datensicherung festgelegt werden. Dazu klicken Sie auf das "+"-Zeichen vor dem Laufwerk D:, und in dem sich öffnenden Verzeichnisbaum sollen Sie das Verzeichnis "Daten" anklicken:



Die Auswahl bestätigen Sie auf der Schaltfläche "Weiter". Sie sehen dann ein Fenster, in dem Sie den Sicherungsumfang festlegen können. Weil dies die erste Datensicherung ist, wählen Sie die erste Möglichkeit mit Mausklick aus ("Alle markierten Dateien").

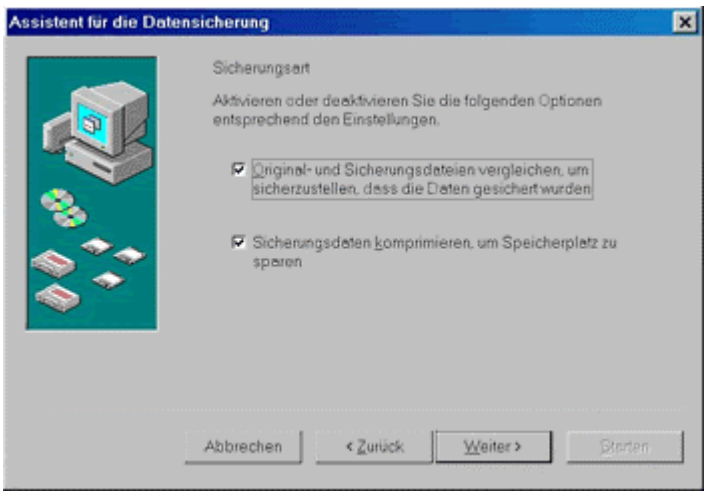


Diese Auswahl müssen Sie auf der Schaltfläche "Weiter" bestätigen.



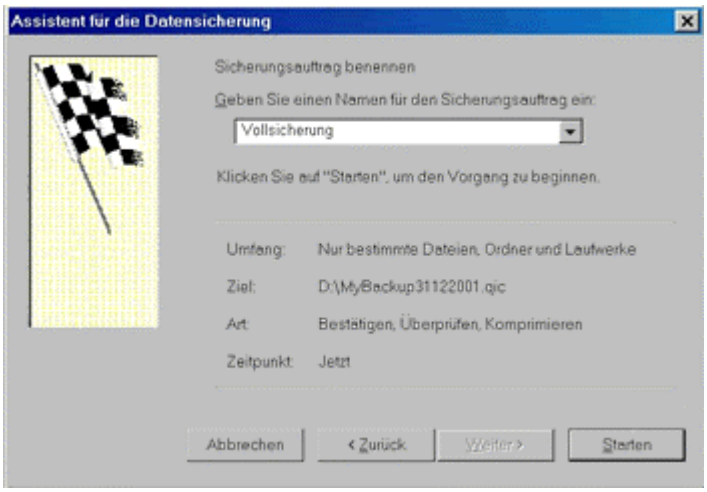
Es erscheint das Fenster, in dem das **Sicherungsziel und der Pfad zu diesem Sicherungsziel** angegeben werden müssen. Weil der Rechner in diesem Beispiel über kein Datensicherungslaufwerk verfügt, kann das Sicherungsziel im Auswahlmenü nicht verändert werden. Das bedeutet, dass die **Daten in eine Datei** gesichert werden. Im Textfeld kann nun die Datei, in die die Datensicherung geschrieben werden soll, angegeben werden. Die Datei muss immer mit .qic enden. Auch einen neuen Pfad können Sie festlegen. Dazu müssen Sie auf den Schalter mit dem Verzeichnissymbol klicken und dann ggf. ein neues Verzeichnis auswählen. In diesem Beispiel erfolgt die Datensicherung in die Datei **MyBackup31122001.qic**, die direkt auf dem Laufwerk D: angelegt werden soll. Der vorgeschlagene Name "MyBackup" ist in dem Beispiel um die Datumsangabe 31122001 erweitert worden. Das erleichtert ein wenig den Umgang mit Backup-Dateien, wenn diese auch das Erstellungsdatum im Namen enthalten.

Diese Auswahl müssen Sie auf der Schaltfläche "Weiter" bestätigen.



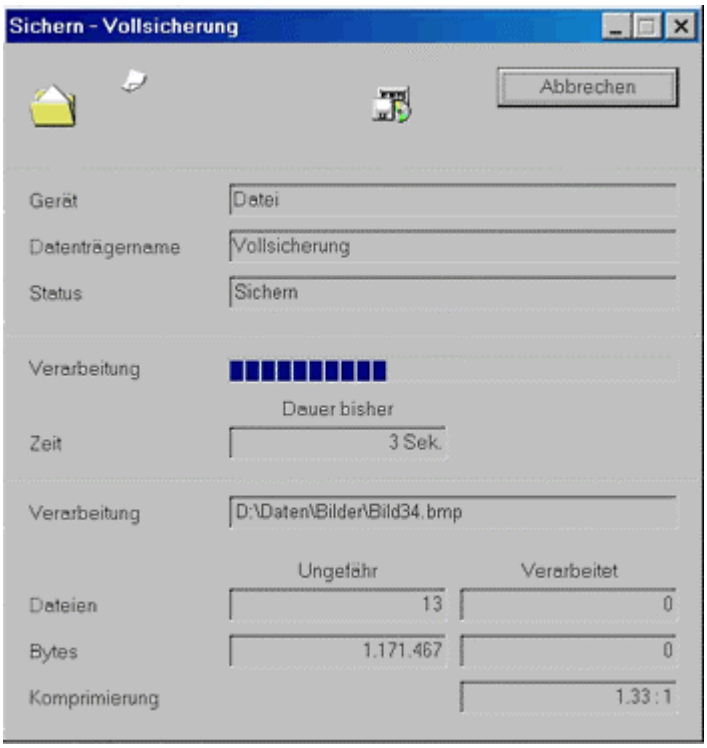
In dem sich dann öffnenden Fenster können Sie festlegen, ob die Original- und Sicherungsdateien verglichen werden sollen. So kann man sicherstellen, dass die Datensicherung ordnungsgemäß erfolgt ist. Weiterhin können Sie festlegen, dass die

Sicherungsdaten komprimiert werden sollen. Das spart Speicherplatz. Empfehlenswert ist es, beide Optionen aktiviert zu lassen. Einziger Nachteil ist, dass die Datensicherung etwas länger dauert.
Indem Sie die Schaltfläche "Weiter" anklicken, bestätigen Sie die Auswahl.

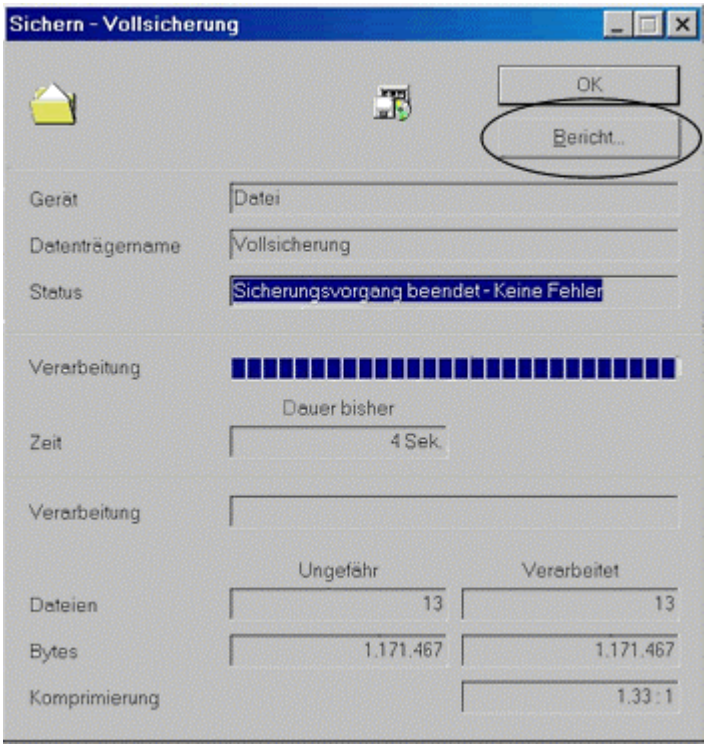


In dem sich dann öffnenden Fenster können Sie einen Namen für den Sicherungsauftrag eingeben. Hier ist der Name "Vollsicherung" eingetragen. Damit kann der Sicherungsauftrag abgespeichert und für spätere Sicherungen wieder verwendet werden. Dies ist insbesondere dann wichtig, wenn sich die zu sichernden Dateien nicht in einem Verzeichnis mit diversen Unterverzeichnissen befinden, sondern über die gesamte Festplatte verstreut sind. Hier noch ein Hinweis: Nicht jede Datensicherungssoftware bietet diese Möglichkeit. So ist auch das Datensicherungstool von Windows 95 nicht in der Lage, solche Auftragsdaten zu speichern. In einem solchen Fall bietet es sich an, wie in diesem Beispiel alle Dateien, die in die Datensicherung einbezogen werden sollen, in einem Verzeichnis mit diversen Unterverzeichnissen zu speichern. Wenn Sie jetzt die Datensicherung starten wollen, klicken Sie auf "Starten".

Während der Datensicherung sehen Sie dieses Fenster:

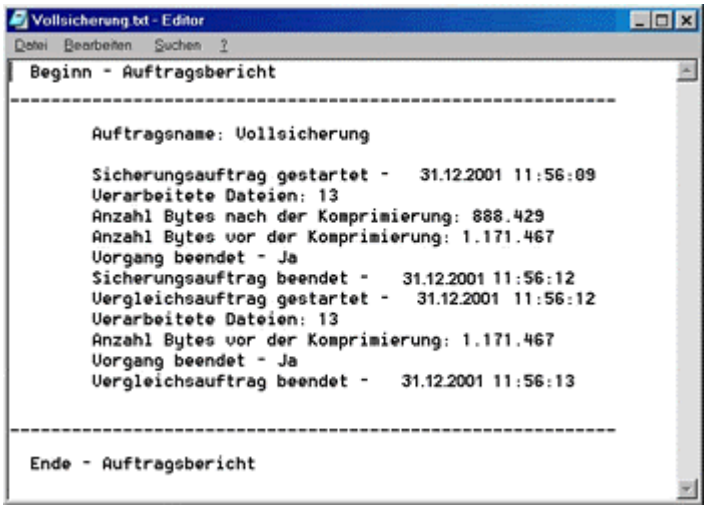


Sobald die Datensicherung beendet ist, öffnet sich ein Fenster, um dies anzuzeigen. Danach kann nur die Schaltfläche "OK" angeklickt werden. Im nächsten Fenster, gibt es eine Schaltfläche "Bericht ...".



Nach jeder Datensicherung sollten Sie diese Schaltfläche anklicken. Dadurch öffnet sich ein Fenster, das einen Bericht enthält, in dem auch Fehler dokumentiert werden,

wenn es welche gibt:



Nach Überprüfung des Berichts können Sie das Datensicherungsprogramm beenden. Die Datei **D:\MyBackup31122001.qic sollten Sie nun auf einem externen Datenträger speichern**. Im Beispiel ist diese Datei 5,89 MB groß, so dass sich hier zum Beispiel die Sicherung auf einer CD-ROM anbietet, insofern Ihr Rechner über einen CD-Brenner verfügt. Danach kann die Datei "MyBackup31122001.qic" auf dem Laufwerk D: gelöscht werden.

Inkrementelle Datensicherung bei Windows 98

Für die inkrementellen Datensicherungen, die nach jeder Benutzung des Rechners durchgeführt werden sollen, müssen Sie einen neuen Datensicherungsauftrag anlegen. Dazu verfahren Sie so, wie zuvor beschrieben. Nur bei der Festlegung des Datensicherungsumfangs ist diesmal die Option "Neue und geänderte Dateien" zu wählen.

Anschließend wählen Sie das Sicherungsziel und die Sicherungsart wie bei der Volldatensicherung. Den Sicherungsauftrag, der nun erstellt werden muss, nennen Sie

zum Beispiel "**inkrementell**".

Alles andere geht wie bei der Vollsicherung.

Nach Abschluss der inkrementellen Datensicherung wird in diesem Beispiel die Datei MyBackup02012002.qic angelegt. Sie befindet sich auf Laufwerk D: und muss noch auf andere Datenträger kopiert werden. Bei kleinen Datenmengen auf Diskette.

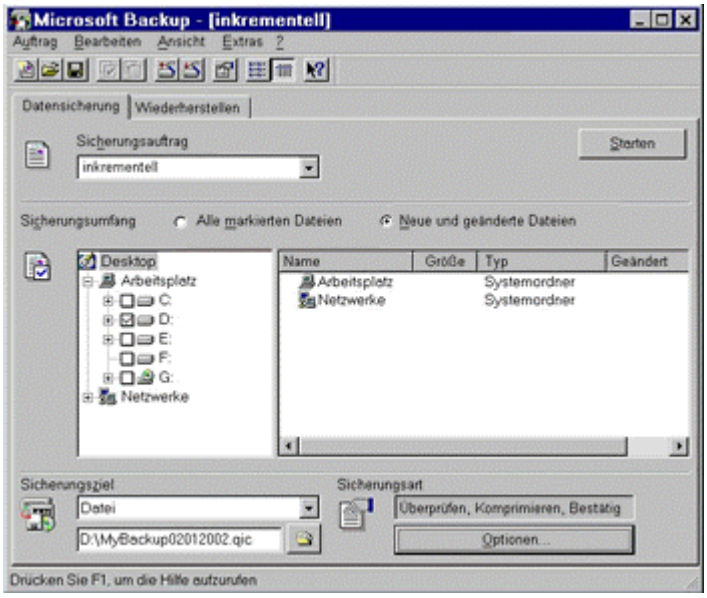
Bei allen weiteren Datensicherungen wählen Sie nach Start des Programms die Option "Einen vorhandenen Sicherungsauftrag öffnen" aus.

Nach Bestätigung auf der Schaltfläche "OK" öffnet sich ein Fenster.

Hier können Sie den Sicherungsauftrag auswählen: Im Beispiel hier der Sicherungsauftrag "Vollsicherung" und der Sicherungsauftrag "inkrementell" für die inkrementelle Datensicherung.

Die Auswahl bestätigen Sie durch "Öffnen" auf der Schaltfläche.

Danach öffnet sich dieses Fenster:



Hier lassen sich noch einmal alle Einstellungen verändern. Unten links können Sie einen neuen Namen für die Datei festlegen, in die die Datensicherung geschrieben wird. Die Datensicherung beginnt nach Mausklick auf die Schaltfläche "Starten".

Die Wiederherstellung von Daten bei Windows 98

Wie sehr sich die Sicherung von Daten lohnt, merken Sie, wenn zum Beispiel Dokumente plötzlich verschwunden sind, eine Anwendung, die Sie doch schon hundertmal erfolgreich ausgeführt haben, nicht mehr klappt, Symbole auf dem Desktop fehlen oder Ihre Festplatte sich aus irgendwelchen Gründen verabschiedet hat.

Wenn alles weg ist

Sollte der ganze Datenbestand auf der Festplatte vernichtet sein, ist es egal, ob ein Totalausfall der Platte, ein versehentlich formatiertes Datenlaufwerk oder ein Virus schuld ist. In diesem Augenblick ist einzig und allein die Wiederherstellung der verlorenen Daten das Thema.

Wenn Sie Ihre Daten regelmäßig gesichert haben, können Sie in diesem Fall die Dateien von Ihren externen Speichermedien - den Disketten, CD-ROMs oder DVDs - zurück ins Standarddatenverzeichnis speichern.

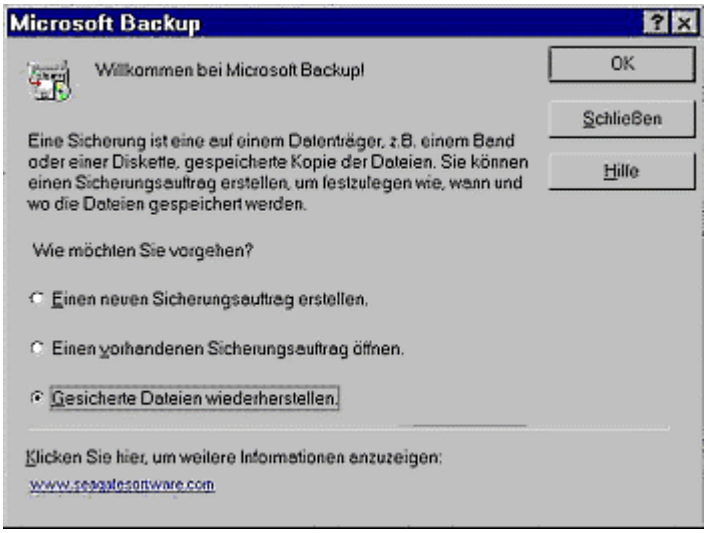
Wenn nicht alles weg ist

1. Volldatensicherung wiederherstellen
2. Inkrementelle Datensicherung einspielen

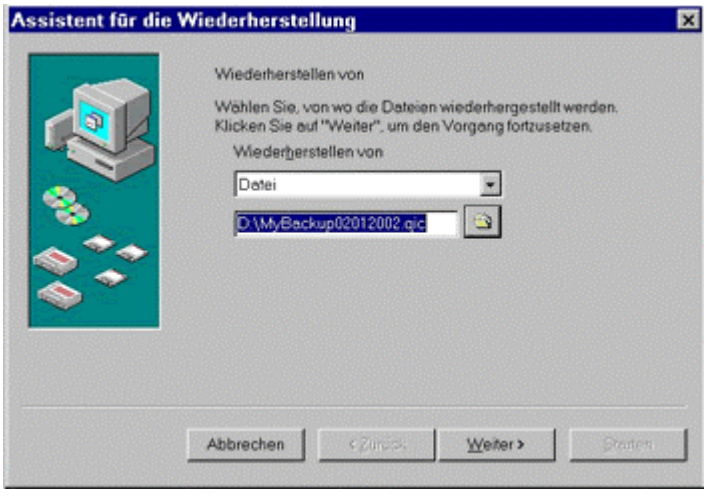
1. Volldatensicherung wiederherstellen

Wenn Sie mehr Glück haben, ist nicht der gesamte Datenbestand weg, sondern es fehlen nur einzelne Dateien. Dabei wollen Sie natürlich möglichst viele Originaldateien erhalten und die auch nicht überschreiben. Also legen Sie jetzt ein eigenes Verzeichnis an, in das Sie die Dateien aus der Datensicherung zurückspeichern. Der Inhalt dieses Verzeichnisses wird nach Abschluss des Wiederherstellungsprozesses in das eigentliche Verzeichnis der Anwendungsdateien umkopiert.

Für das folgende Beispiel heißt das Verzeichnis "Wiederherstellung" und wurde auf Laufwerk D: angelegt. Dort hinein kopieren Sie später Ihre letzte Volldatensicherung, anschließend alle inkrementellen Datensicherungen. Zunächst klicken Sie nach dem Start des Programms auf die Option "Gesicherte Dateien wiederherstellen" und bestätigen die Auswahl auf der Schaltfläche "OK":



Dadurch öffnet sich dieses Fenster:

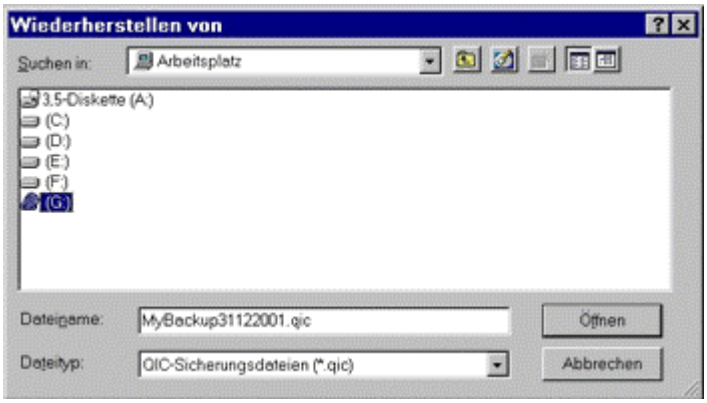


Dort haben Sie zwei Felder. Das obere ermöglicht die Auswahl des Geräts, das zur Datensicherung eingesetzt worden ist. Die vorgegebene Einstellung können Sie aber nur verändern, wenn Ihr Rechner ein Datensicherungslaufwerk hat. In diesem Beispiel

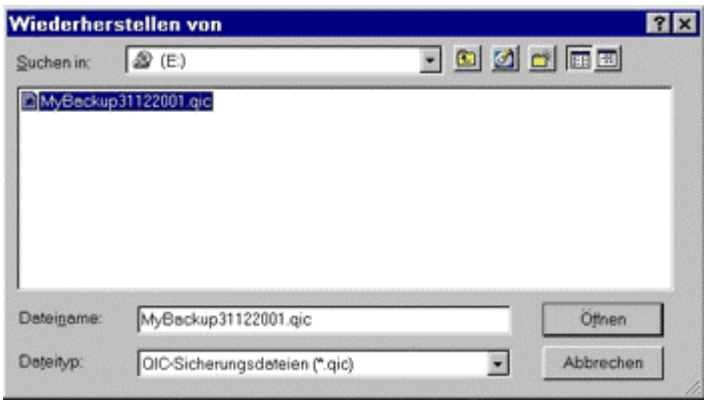
hat er keines, also können Sie die Daten nur aus einer Datensicherungsdatei wiederherstellen.

Im Textfeld unten wird die Datei festgelegt, in der die Datensicherung gespeichert wurde. Standardmäßig erscheint dort immer die zuletzt benutzte Datei. Damit können Sie jetzt nichts anfangen, weil in diesem Beispiel Ihre Datei auf einer CD-ROM liegt. Deshalb müssen Sie dem Rechner den Weg zur CD-Datei weisen, das heißt den Pfad angeben. Dazu klicken Sie auf das Ordnersymbol rechts neben dem Menü.

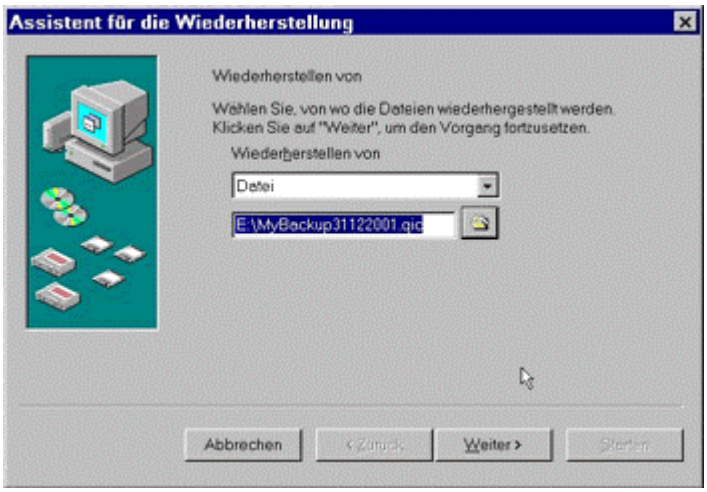
Jetzt öffnen Sie das Fenster für die Auswahl des Laufwerks mit der Sicherungsdatei:



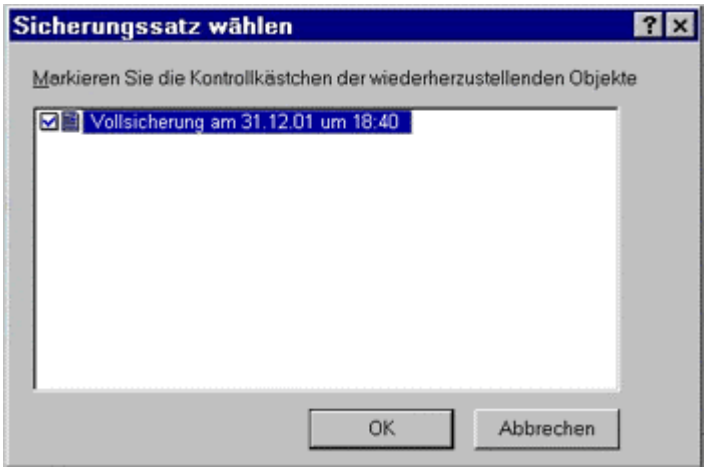
Dort klicken Sie auf das Laufwerk des Datensicherungsmediums und markieren dann die Datei. Im Beispiel hier ist es "MyBackup31122001.qic", gespeichert auf Laufwerk E:, dem CD-ROM-Laufwerk:



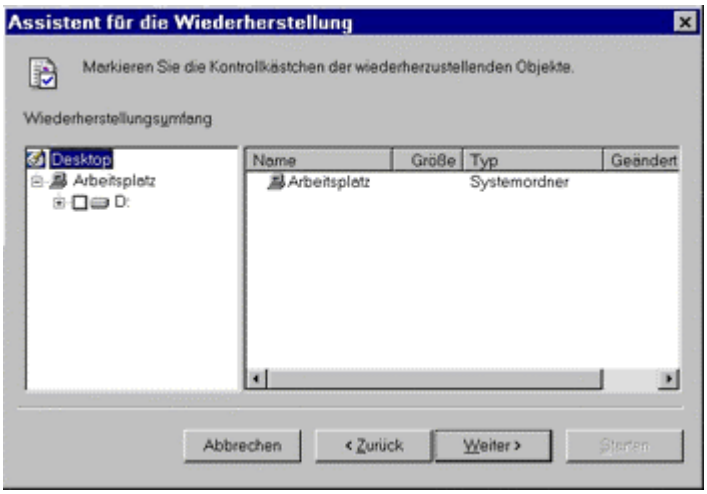
Wenn Sie auf "Öffnen" klicken, gelangen Sie zum Fenster des Wiederherstellungsassistenten. Dort sehen Sie im unteren Menü Ihre gewählte Datensicherungsdatei:



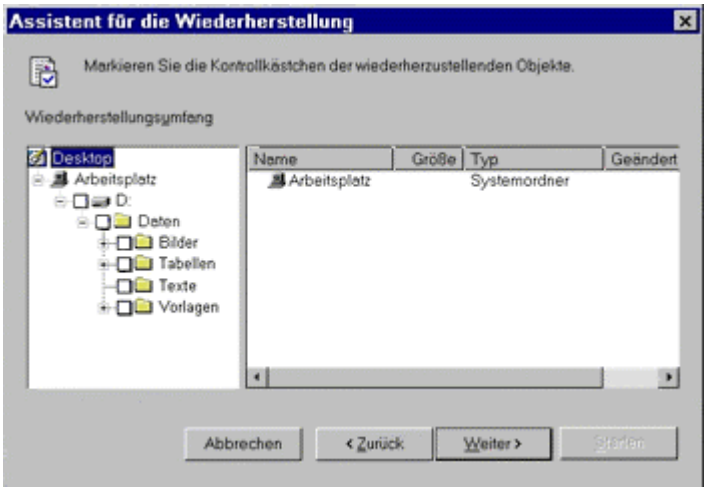
Sie klicken auf "Weiter" und sehen das Fenster für den Datensicherungsauftrag, aus dem die Wiederherstellung erfolgen soll.



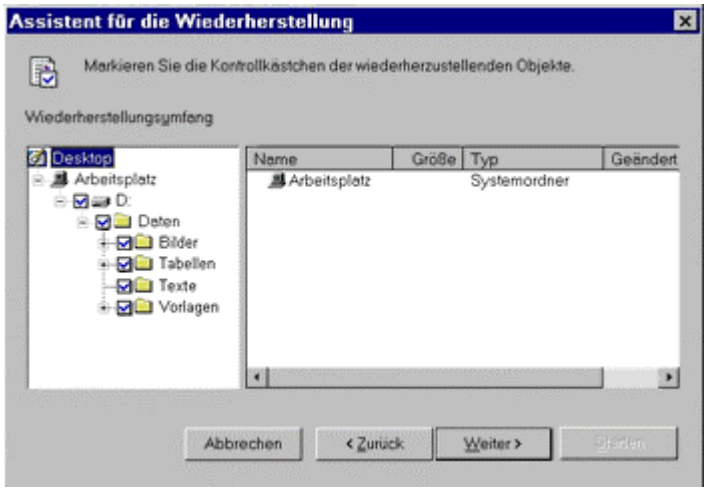
Klick aufs Kästchen oben links. Dort setzt sich ein Häkchen rein, das Ihnen zeigt: Der Auftrag ist erteilt. Ihre Bestätigung auf "OK" öffnet das Fenster mit dem Verzeichnisbaum, der in der Datensicherung gespeichert ist:



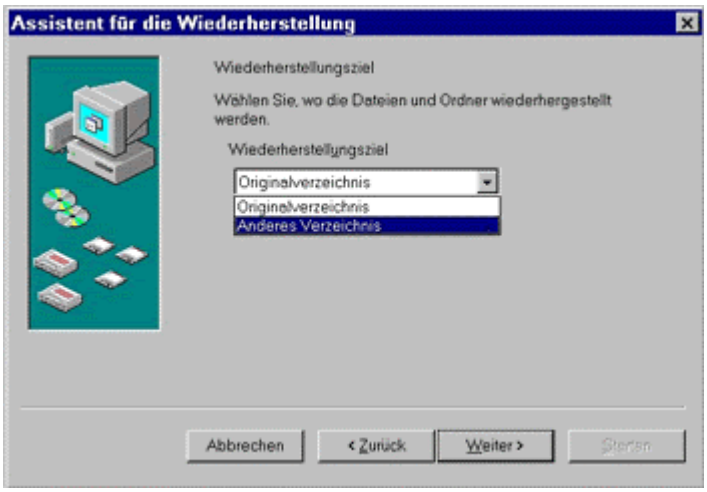
Ein Klick auf das Kreuzchen links neben Laufwerk D: öffnet den Verzeichnisbaum :



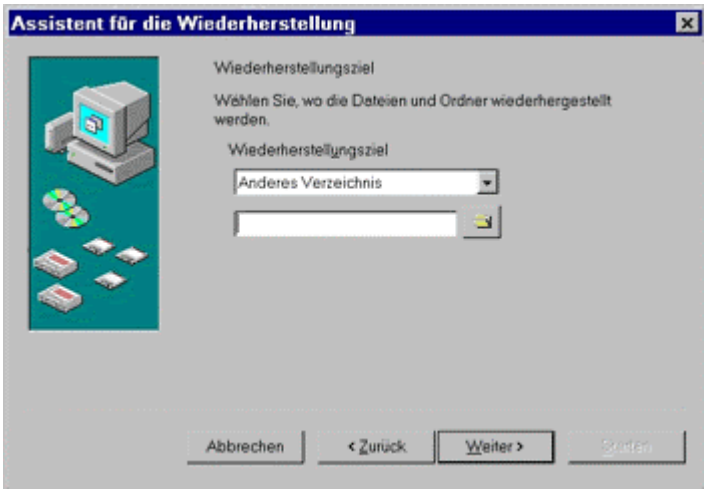
Die Unterverzeichnisse würden angezeigt, wenn Sie die Kreuzchen links neben den Verzeichnissen anklicken. Weil die gesamte Volldatensicherung wiederhergestellt werden soll, nehmen Sie aber das Kästchen neben dem Verzeichnis D:\Daten und öffnen damit das folgende Fenster:



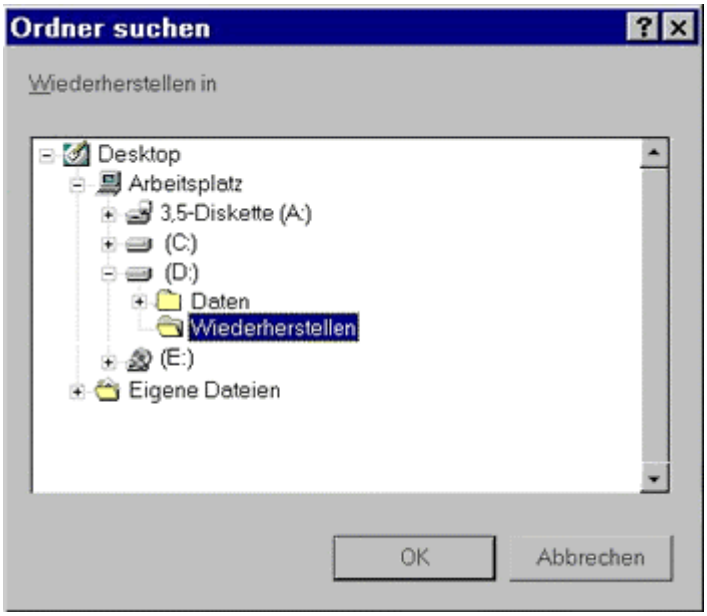
Ihnen fällt sicher auf, dass nicht nur vor dem Verzeichnis D:\Daten ein blaues Häkchen ist, sondern auch vor allen Unterverzeichnissen. Also sind alle Unterverzeichnisse und auch die darin liegenden Daten für die Wiederherstellung markiert worden. Im Kästchen vor dem Laufwerk D: ist ein graues Häkchen, weil für die Wiederherstellung nicht das gesamte Laufwerk, sondern nur ein Verzeichnis mit entsprechenden Unterverzeichnissen ausgewählt wurde. Auf "Weiter" bestätigen Sie nun die Auswahl und sehen dieses Fenster:



Hier müssen Sie das Menü öffnen und sich für "Anderes Verzeichnis" entscheiden. Die Bestätigung auf "Weiter" öffnet eine Variante des Wiederherstellungsassistenten:

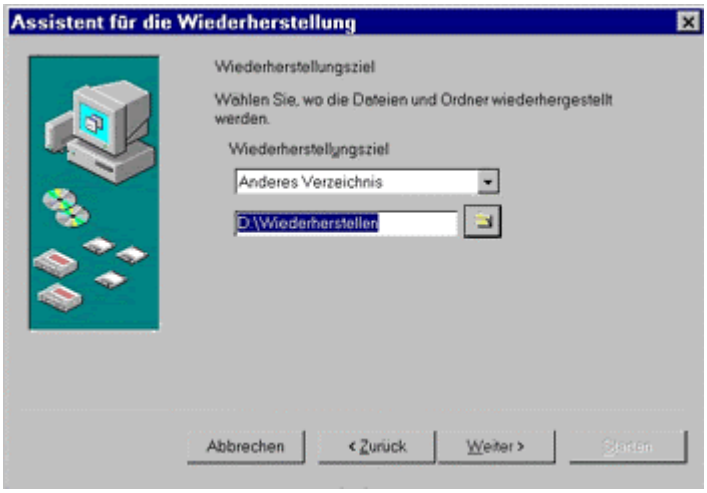


Klick aufs Ordnersymbol rechts neben der leeren Menüzeile macht einen Verzeichnisbaum auf:



Oben suchen Sie das Verzeichnis aus, in das die Dateien aus der Datensicherung eingestellt werden sollen. Für dieses Beispiel haben Sie das Verzeichnis D:\Wiederherstellen angelegt und mit einem Mausklick ausgewählt. Also auf "OK" bestätigen.

- Das nächste Fenster:



Nach dem Klick auf "Weiter" werden Sie nach der Wiederherstellungsart gefragt:

Sie legen fest, was passieren soll, wenn sich die gleiche Datei sowohl in der Datensicherung befindet als auch im Datenverzeichnis, in das die Wiederherstellung erfolgen soll. Wenn Sie die Daten ins Originaldatenverzeichnis zurückspeichern wollen, nehmen Sie die Möglichkeit "Datei auf Datenträger nicht ersetzen (empfohlen)".

Diese Option nützt Ihnen allerdings nichts, wenn Sie gerade eine ältere Version einer zwar vorhandenen, aber versehentlich überschriebenen Datei brauchen. Nicht sinnvoll ist diese Option, beim Wiederherstellen von Datenbeständen über inkrementelle Datensicherungen.

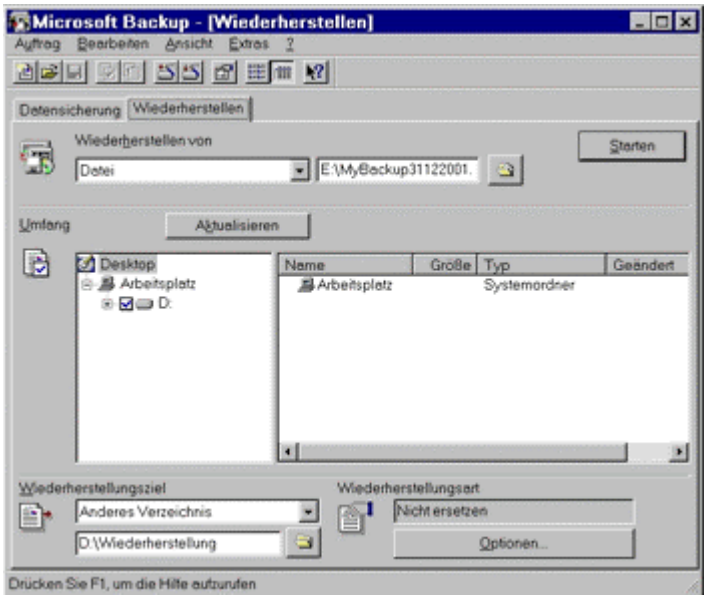
Im Beispiel hier wurde das Verzeichnis gewählt, das für die Wiederherstellung der Dateien angelegt worden ist. Dieses Verzeichnis enthält vor der Wiederherstellung keine Dateien. Deshalb spielen die Optionen für die Wiederherstellung von Dateien jetzt keine große Rolle. Sie ändern die voreingestellte Option also nicht, weil die Wiederherstellung zunächst aus der letzten Volldatensicherung kommen soll. Die Auswahl bestätigen Sie mit Klick auf "Starten" und sehen dann dieses Fenster:

Jetzt den Datenträger auswählen, auf dem sich die Datensicherung befindet. Ihre Bestätigung auf "OK" öffnet ein Wiederherstellungsfenster:

In der Zeile "Verarbeitung" sehen Sie den Prozess des Wiederherstellens. Dieser ist abgeschlossen sobald die Zeile blau gefüllt ist.

Auch jetzt sollten Sie - wie beim Datensicherungslauf - das Protokoll überprüfen. Klicken Sie auf "Bericht" oben rechts, und schon ist er da:

Die Wiederherstellung der Dateien aus der letzten Volldatensicherung ist abgeschlossen. Sie sehen dieses Fenster:



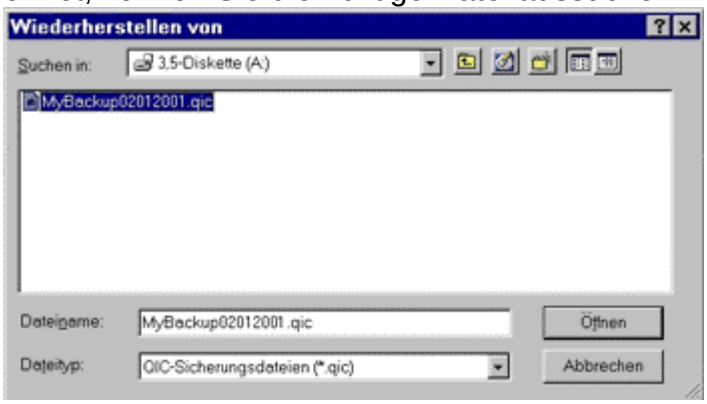
Wenn sich Ihre Dateien nach der letzten Volldatensicherung verändert haben, müssen Sie jetzt noch die inkrementellen Datensicherungen einspielen. Haben Sie keine inkrementellen Datensicherungen vorgenommen, sind veränderte Dateien nicht mehr herstellbar, und Sie müssen sich mit dem Zustand der letzten Volldatensicherung begnügen.
Wenn doch, geht's weiter.

2. Inkrementelle Datensicherungen einspielen

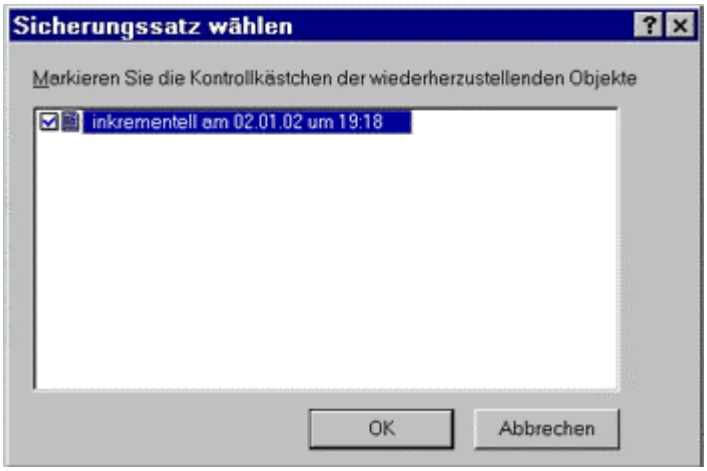
Jetzt müssen Sie die inkrementellen Datensicherungen wiederherstellen - in der Reihenfolge, in der sie angelegt worden sind. Im gezeigten Beispiel sind die Datensicherungen auf Diskette. Nun suchen Sie die erste inkrementelle Datensicherung nach der letzten Volldatensicherung. Sie wählen den Datensatz mit der inkrementellen Sicherung im oben dargestellten Fenster aus.

Anschließend öffnet sich folgendes Fenster, wo Sie auf das Verzeichnissymbol im zweiten Auswahlfensterchen oben rechts klicken. Im Verzeichnisbaum, der sich dann

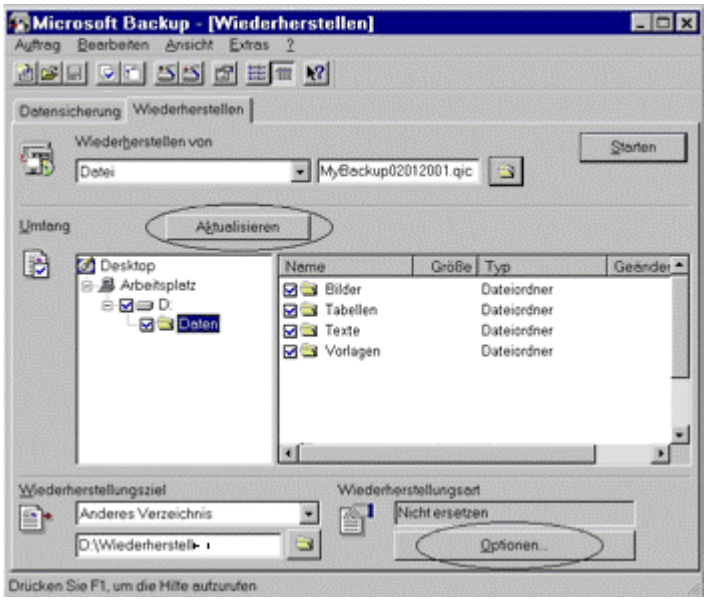
öffnet, können Sie die richtige Datei aussuchen:



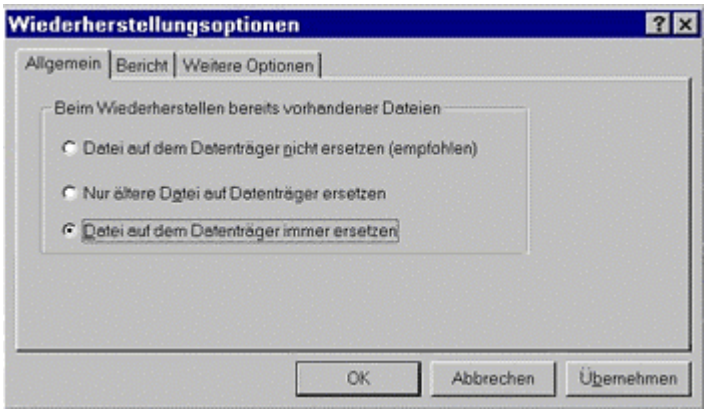
Für das Beispiel hier klicken Sie aufs Laufwerk A:, weil Diskette, und dann auf die Datei "MyBackup02012001.qic". Die Bestätigung auf "Öffnen" führt zu diesem Fenster:



Die Datensicherung, die Sie zur Wiederherstellung nutzen wollen, markieren Sie mit der Maus im linken Kästchen. Blaues Häkchen, Klick auf "OK", neues Fenster, wie gehabt:

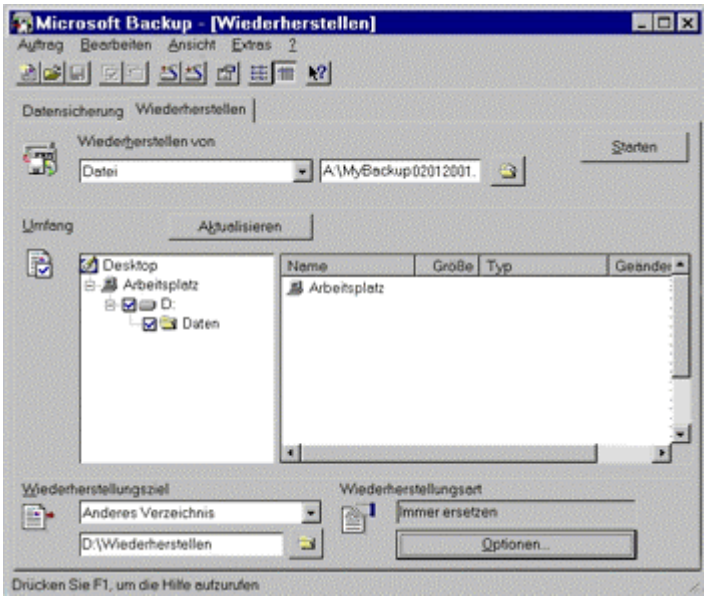


Klick auf "Aktualisieren" und aufs Kreuzchen vor dem Laufwerk D: öffnet wieder den Verzeichnisbaum. Klick aufs leere Kästchen vor dem Verzeichnis D:\Daten. Dass das hier schon gemacht ist, sehen Sie am blauen Häkchen oben. Jetzt auf Schaltfläche "Optionen" - neues Fenster:



Sie haben die Option "Datei auf dem Datenträger immer ersetzen" ausgewählt, weil im Beispiel hier ein gesamter Datenbestand wiederhergestellt werden soll. Bei der Datensicherung haben Sie als Volldatensicherung alle Dateien gesichert. Und als inkrementelle alle neuen und geänderten Dateien. Bei der Wiederherstellung wurde der Zustand zum Zeitpunkt der Volldatensicherung rekonstruiert. Durch Einspielen der inkrementellen Datensicherungen sind die jeweils aktuelleren Zustände wieder auf der Festplatte. Und Sie haben die Wiederherstellung in einem eigenen Verzeichnis vollzogen. Das alles ermöglichte eben die Option, die Sie oben ausgesucht haben. Hätten Sie das alles nicht gemacht, könnten in den inkrementellen Datensicherungen aktuellere Dateien sein, die nicht wiederhergestellt werden, weil bereits ein älteres Exemplar vorhanden ist.

Sie bestätigen jetzt Ihre Auswahl mit Klick auf "OK" und öffnen damit dieses Fenster:



Für die Wiederherstellung der Daten genügt ein Klick auf "Starten", der dann auch zu diesem Fenster führt:

Jetzt mit der Maus den Datenträger auswählen und die Auswahl auf "OK" bestätigen.

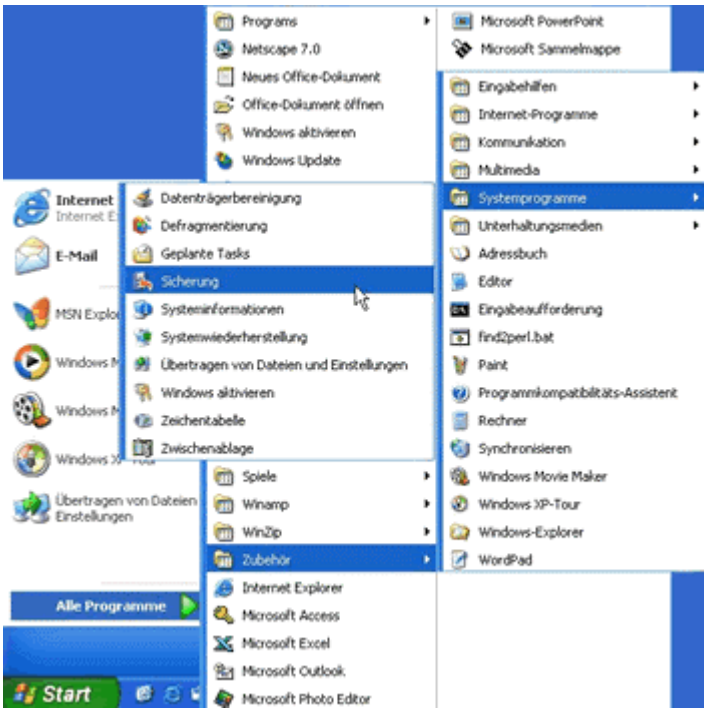
Wenn die Wiederherstellung beendet ist, haben Sie es mit dem nächsten und letzten Fenster hinter sich:

Und zum guten Schluss sollten Sie sich noch den Bericht dieser Wiederherstellung durch einen Klick auf "Bericht" oben rechts anzeigen lassen. Nun haben Sie es geschafft!

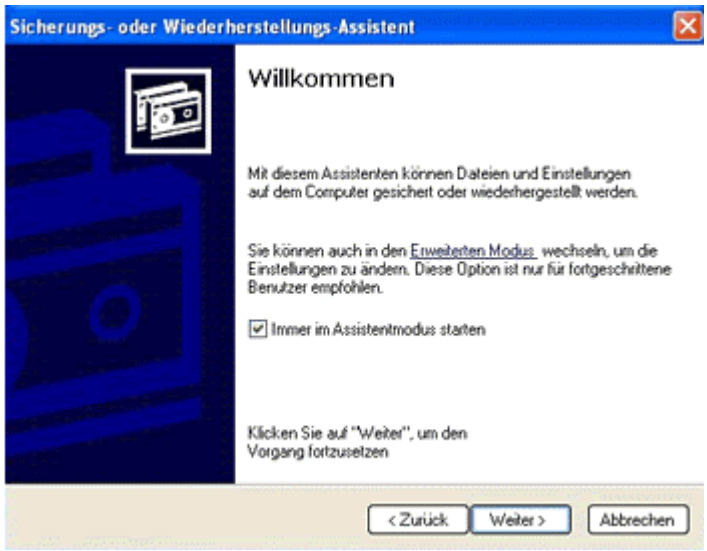
Quelle: http://www.bsi-fuer-buerger.de/03/03080401.htm

Volldatensicherung bei Windows XP

Zunächst installieren Sie die Software, wenn sie nicht schon auf Ihrem PC ist. Dazu gehen Sie im Startmenü auf den Menüpunkt "Alle Programme", dann auf "Zubehör". Es öffnet sich eine neue Schaltfläche, dort wählen Sie "Systemprogramme" aus und anschließend klicken Sie auf "Sicherung".

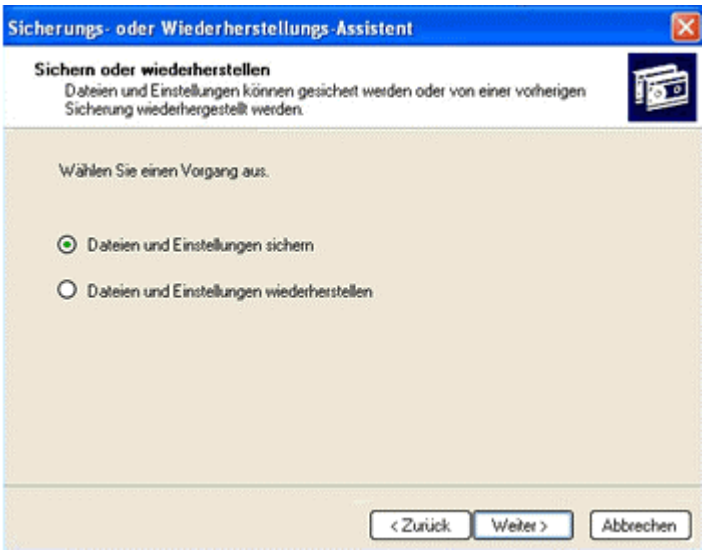


Jetzt sehen Sie den Sicherungs- oder Wiederherstellungs-Assistenten.

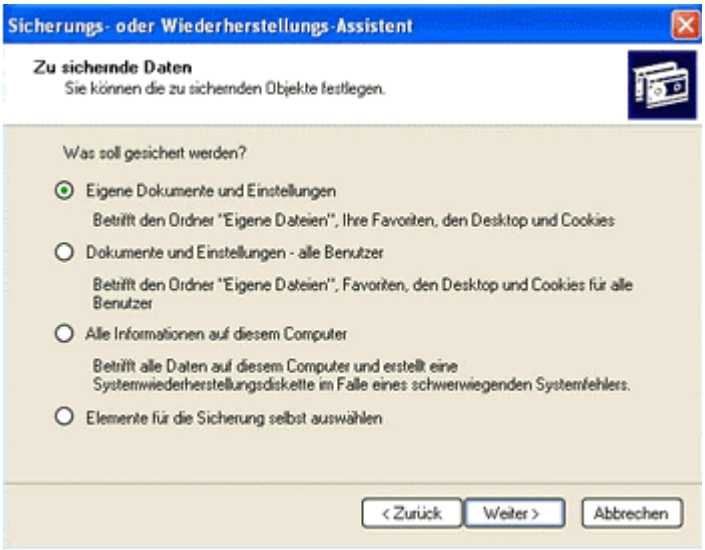


Für normale Benutzer empfiehlt es sich, immer im Assistent-Modus zu starten, deshalb setzen Sie ein Häckchen in diesem Feld und drücken auf "Weiter".

Im nun folgenden Fenster müssen Sie sich entscheiden, ob Sie Daten sichern oder wiederherstellen wollen. Sie wollen aber erst einmal Daten sichern, denn wo zunächst nichts gesichert wurde, lässt sich später natürlich auch nichts mehr wiederherstellen.



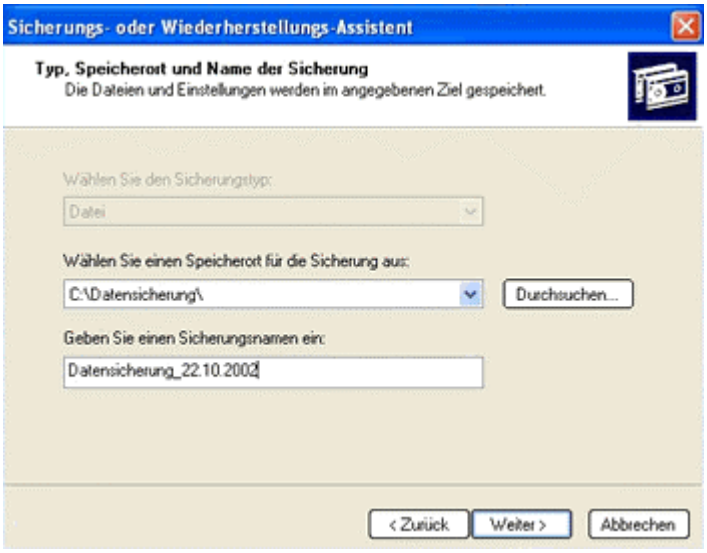
Mit einem Klick auf "Weiter" gelangen Sie zum nächsten Fenster.



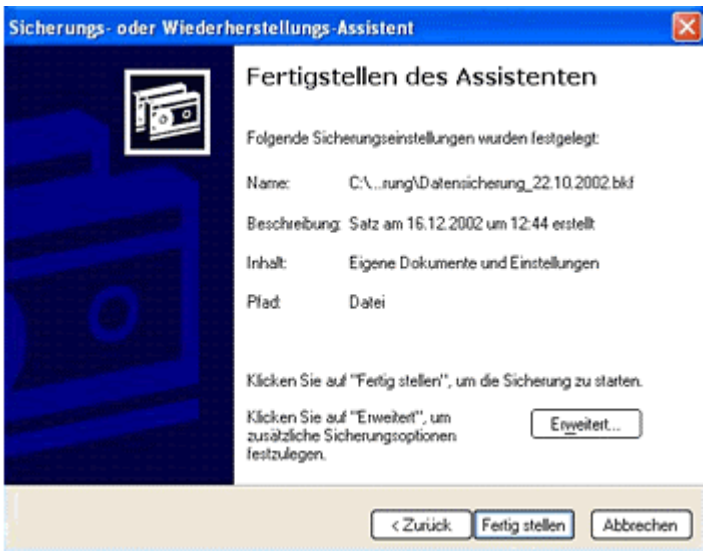
Dort bestimmen Sie, was Sie genau sichern möchten. Im Beispiel werden nur die Dokumente und Einstellungen eines Benutzers gesichert. Es lassen sich jedoch auch sämtliche auf dem Computer gespeicherte Informationen sichern. Fortgeschrittene Benutzer können auch einzelne Elemente auswählen. Ihre Auswahl bestätigen Sie mit "Weiter".

Jetzt müssen Sie entscheiden, wo Sie Ihre Daten sichern möchten. Ort und Namen können Sie beliebig auswählen. Wählen Sie für Ihre Datensicherung einen "sprechenden" Namen aus. Handelt es sich um einen Dateinamen wird die Erweiterung

.bkf automatsich angehängt.



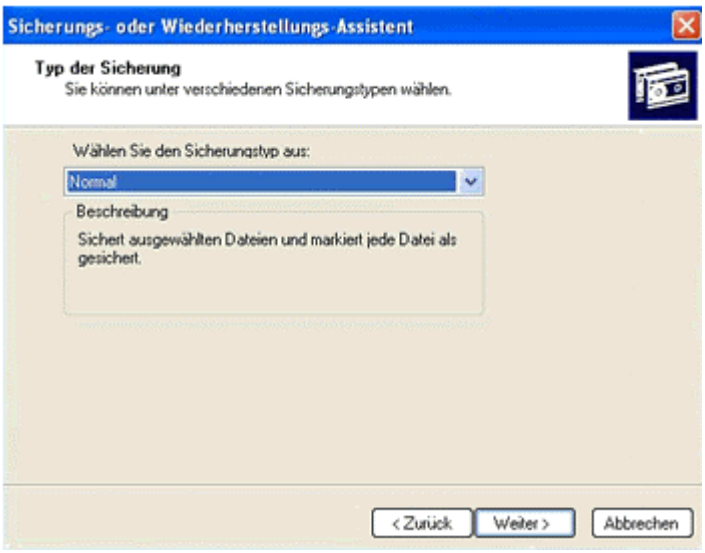
Durch den Klick auf "Weiter" öffnet sich das nächste Fenster.



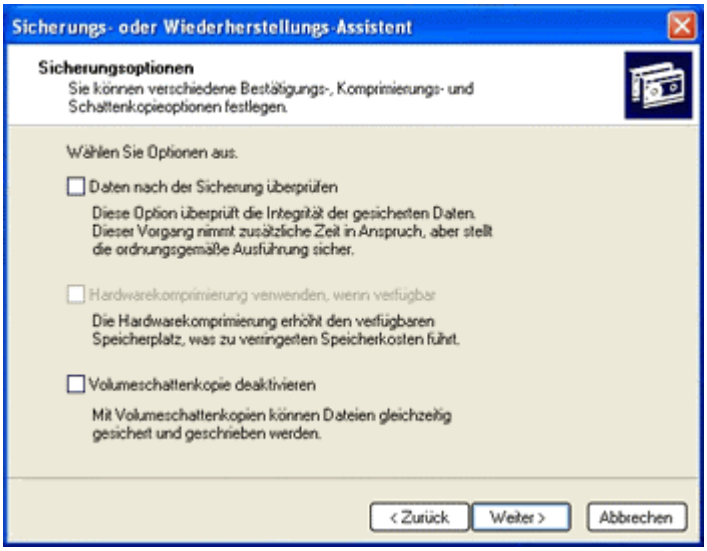
Sie sehen nun alle festgelegten Sicherungseinstellungen auf einen Blick. Um die Sicherung sofort zu starten klicken Sie auf "Fertig stellen".

Möchten Sie weitere Details bestimmen, zum Beispiel wenn Sie die Datensicherung nicht sofort durchführen möchten, klicken Sie auf "Erweitert".

In diesem Fenster können Sie den Typ der Datensicherung bestimmen.



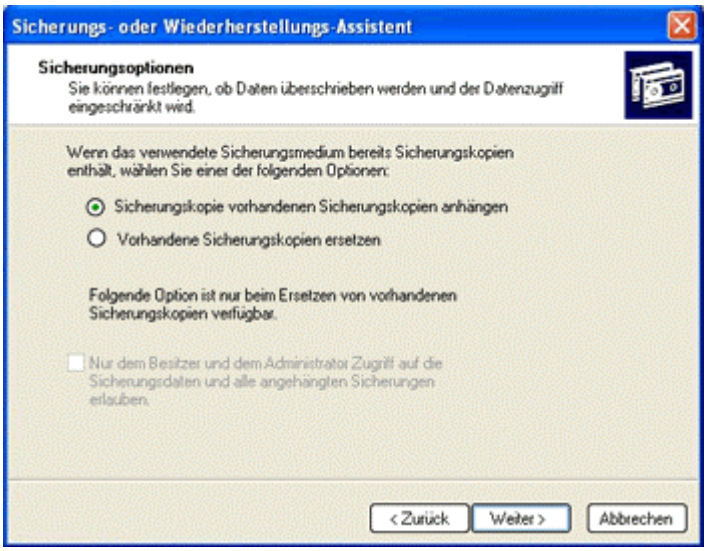
Es gibt die Typen: Normal, Kopieren, Inkrementell, Differenziell oder Täglich. Normale Sicherung heißt, dass sämtliche ausgewählte Dateien und Order gesichert werden. Im Falle eines Datenverlustes lassen sich die Daten schneller wiederherstellen, wenn sie mit der "Normalen Sicherung" gesichert wurden, weil es sich dabei um die aktuellsten Dateien handelt und dadurch die Wiederherstellung mehrerer Sicherungsaufträge nicht erforderlich ist. Im Beispiel wird deshalb die Datensicherung ausgewählt und auf "Weiter" geklickt.



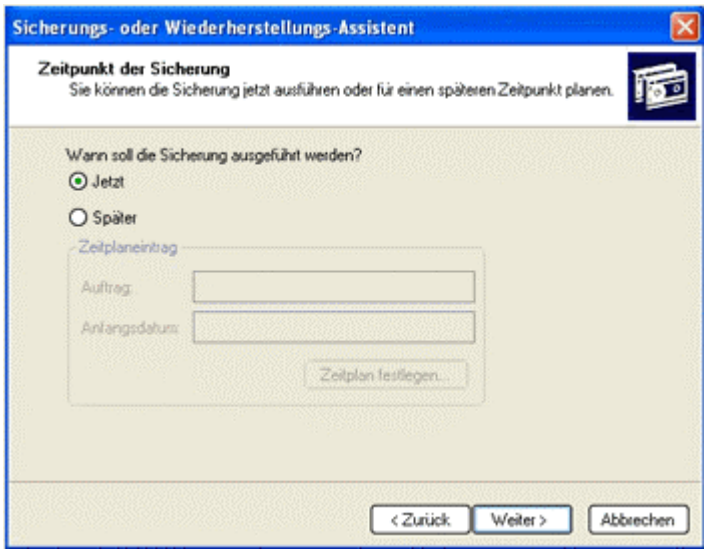
Im Fenster "Sicherungsoptionen" wird geprüft, ob alle Dateien richtig gesichert wurden. Dabei vergleicht das Datensicherungsprogramm, ob Sicherungs- und Ursprungsdaten identisch sind. Diese Option ist empfehlenswert und deshalb wird im Beispiel auch "Daten nach der Sicherung überprüfen" ausgewählt. Wenn Ihr Rechner nicht über ein Bandgerät verfügt, dass die Hardwarekomprimierung unterstützt, wird der zweite Punkt" abgeblendet und ist nicht wählbar. Das Kästchen "Volumenschattenkopie" ermöglicht die Sicherung von Daten, selbst wenn diese gerade bearbeitet werden. Wenn es bei Ihnen nicht abgeblendet dargestellt wird (normalerweise verwendet das Sicherungsprogramm diese Option standardmäßig), dann sollten Sie dieses Kästchen

ebenfalls anklicken. Dann geht's mit "Weiter" weiter.

Der Sicherungs-Assistent sagt Ihnen im nächsten Fenster, dass Sie die Wahl haben, die Daten an die bereits vorhandenen Sicherheitskopien anzuhängen oder aber alle vorhandenen Sicherungskopien zu überschreiben.



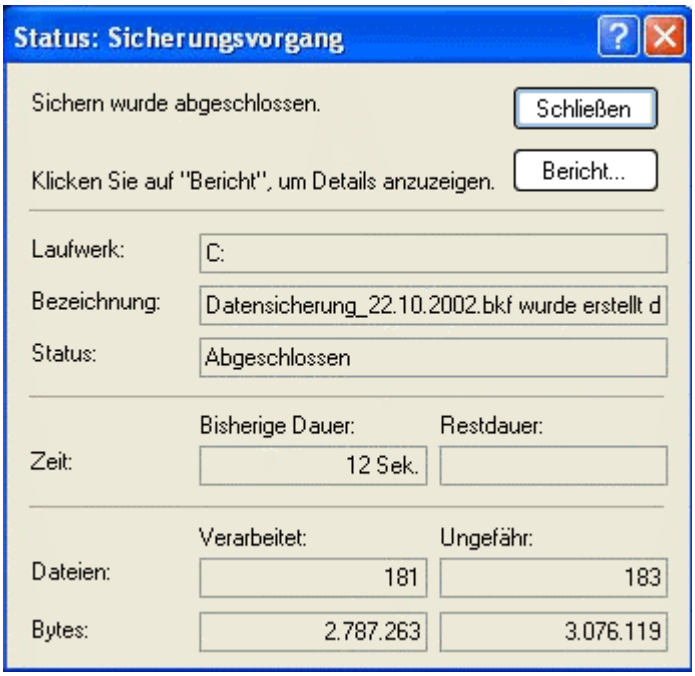
Für was Sie sich entscheiden bleibt Ihnen überlassen, im Beispiel wird die erste Möglichkeit gewählt und mit "Weiter" bestätigt.



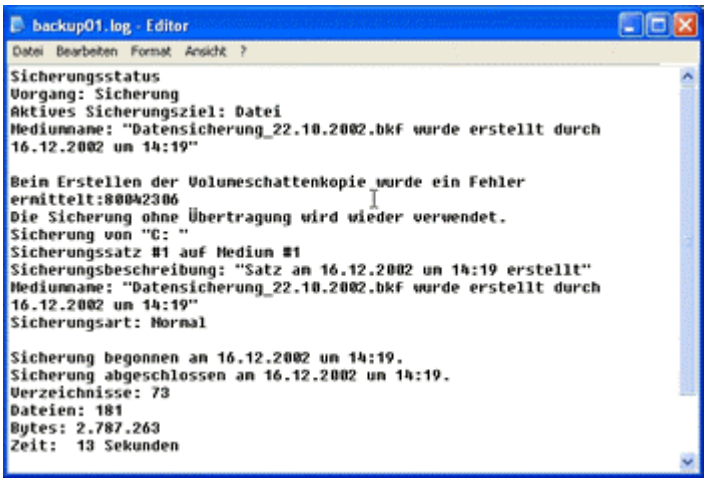
Jetzt können Sie auch noch den Zeitpunkt für die Durchführung der Datensicherung einstellen. Wenn Sie "später" wählen, müssen Sie einen Auftragsnamen und das Startdatum angeben. Ihre Auswahl bestätigen Sie in beiden Fällen mit "Weiter". Wenn Sie nun den Sicherungsprozess abschließen wollen, zeigt Ihnen der Assistent die Einstellungen "Fertigstellen des Assistenten an". Sie können dann die Sicherung sofort starten.

Egal, ob Sie die erweiterten Einstellungen gewählt haben oder aber direkt mit der

Datensicherung begonnen haben, sobald die Datensicherung abgeschlossen wurde, wird der Statusbericht angezeigt.



Mit einem Mausklick auf die Schaltfläche "Schließen" wird der Datensicherungsvorgang beendet. Sicherheitshalber sollte man jedoch einen Klick auf "Bericht ... " durchführen, um sich weitere Details zum Datensicherungsvorgang anzeigen zu lassen. Das ist sinnvoll um eventuelle Fehler, die bei der Datensicherung auftreten können, zu entdecken. Wenn Sie den Bericht überprüft haben, können Sie das Datensicherungsprogramm beenden.

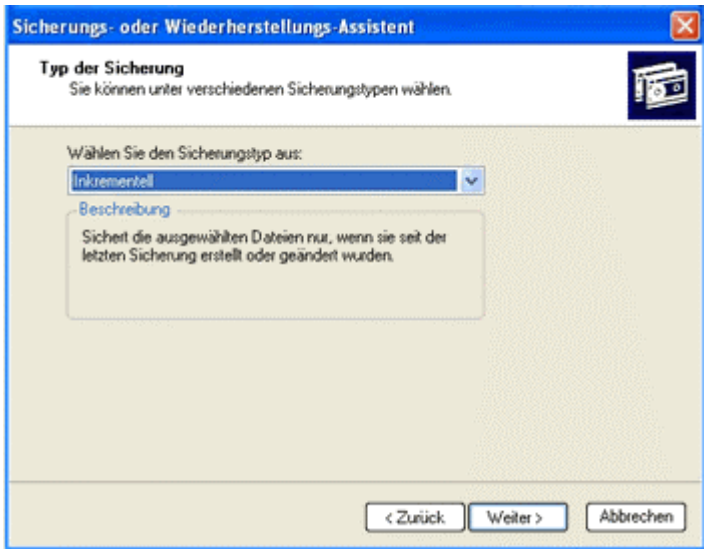


Die Datei - im Beispiel "Datensicherung_22.10.2002.bkf" - sollten Sie jetzt auf einem externen Datenträger speichern. Ist sie größer als 1,44 MB, dann bietet sich die Sicherung auf einer CD-ROM an.

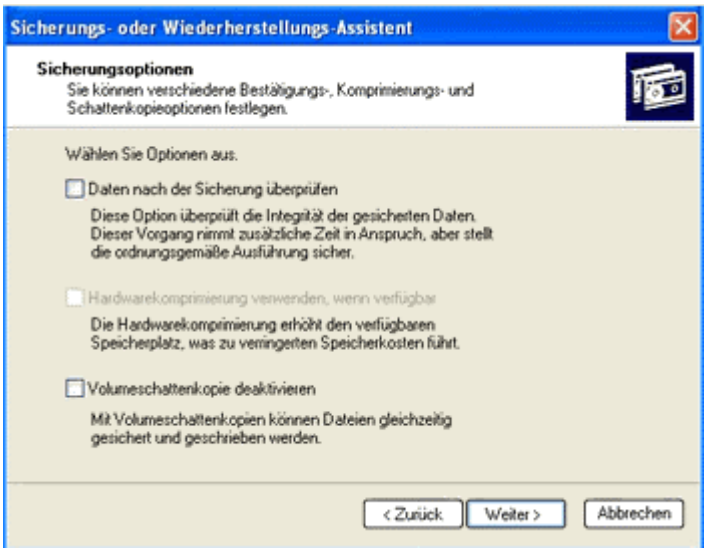
Inkrementelle Datensicherung bei Windows XP

Für die inkrementelle Datensicherung, die in regelmäßigen Abständen wiederholt werden sollte, ist es notwendig, dass Sie zuvor eine Volldatensicherung durchgeführt haben. Anschließend verfahren Sie wie folgt: Sie legen bei der die inkrementellen Datensicherungen einen neuen Datensicherungsauftrag an. Das machen Sie genauso wie bei der Volldatensicherung bis Sie zum Fenster "Fertigstellen des Assistenten" gelangen.

Bevor Sie den Datensicherungs-Assistenten jedoch fertigstellen, klicken Sie auf "Erweitert...".

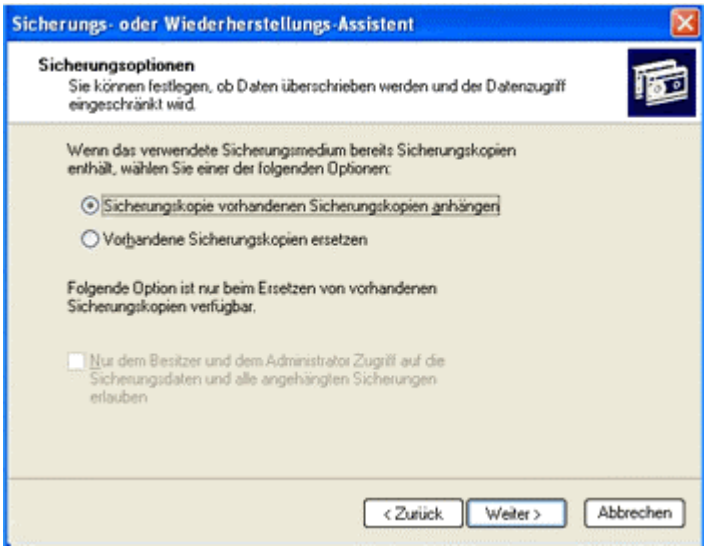


Hier wählen Sie nun den Punkt "Inkrementell" aus.

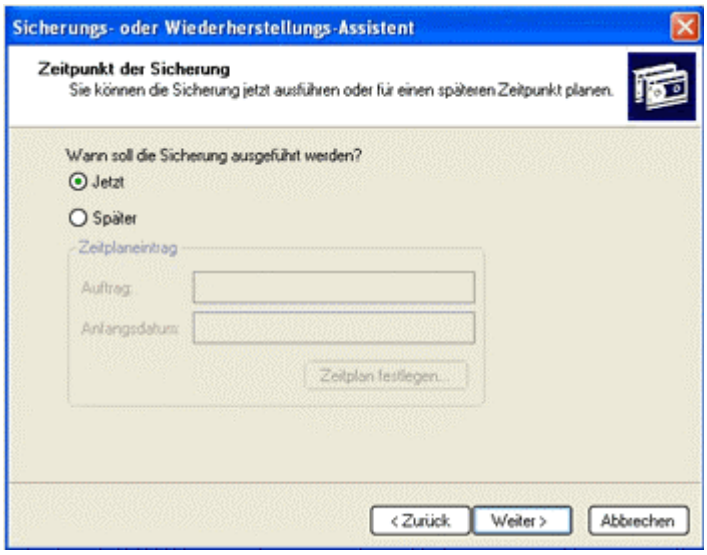


Nun können Sie - wie bei der Volldatensicherung - wieder verschiedene Optionen festlegen. Dann klicken Sie auf "Weiter".

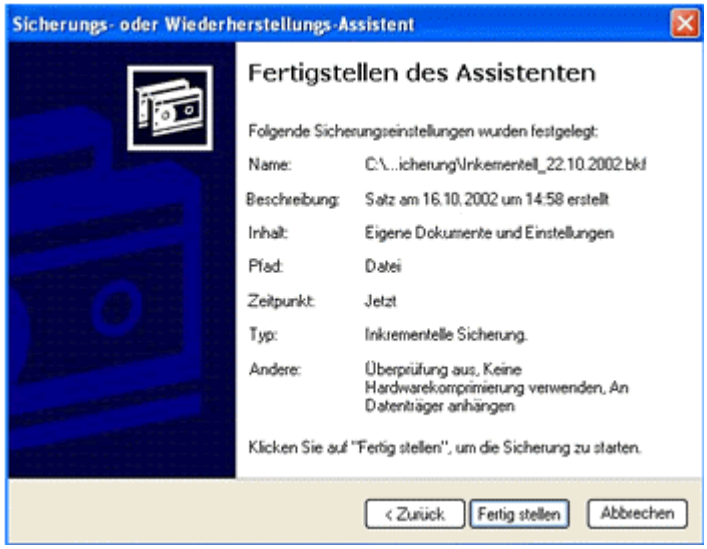
Der Sicherungs-Assistent sagt Ihnen im nächsten Fenster, dass Sie die Wahl haben, die Daten an die bereits vorhandenen Sicherheitskopien anzuhängen oder aber alle vorhandenen Sicherungskopien zu ersetzen.



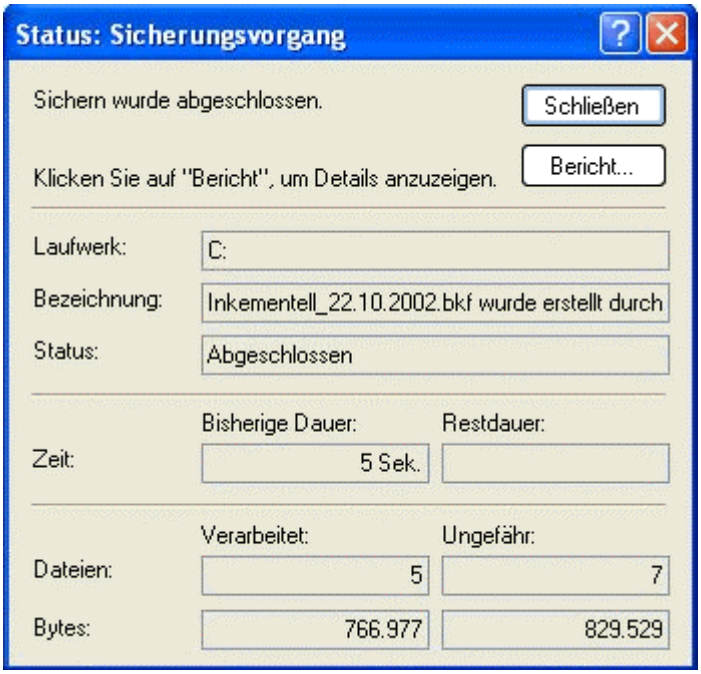
Für was Sie sich entscheiden bleibt Ihnen überlassen, im Beispiel wird die erste Möglichkeit gewählt und mit "Weiter" bestätigt.



Jetzt können Sie auch noch den Zeitpunkt für die Durchführung der Datensicherung einstellen und Ihre Auswahl mit "Weiter" bestätigen.



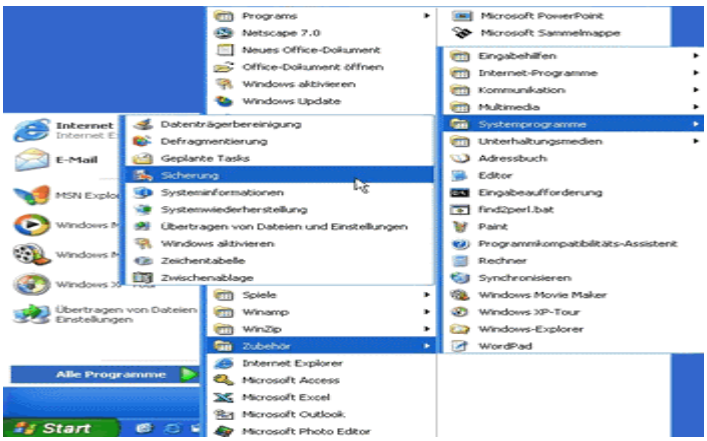
Erneut sehen Sie in diesem Fenster alle Ihre gewählten Einstellungen, die sich mit einem Klick auf "Fertig stellen" bestätigen.



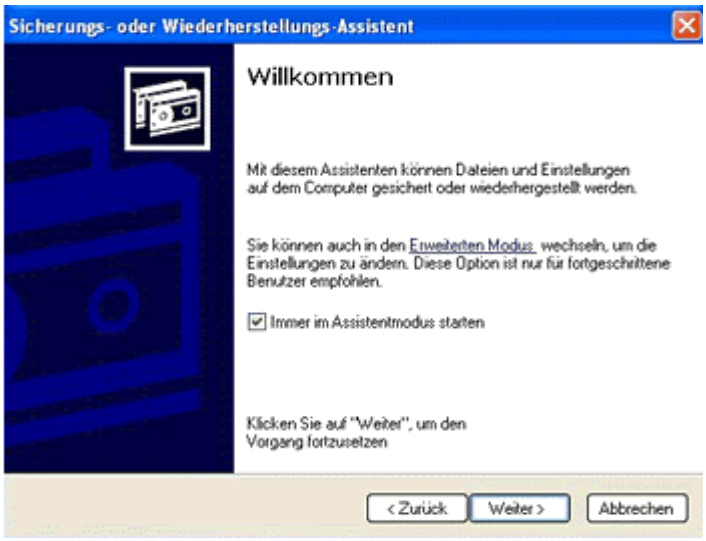
Sobald die Datensicherung abgeschlossen wurde, wird der Statusbericht angezeigt. Diesen können Sie schließen oder sich die Details durch einen Klick auf "Bericht ... " anzeigen lassen. Das ist sinnvoll um eventuelle Fehler, die bei der Datensicherung auftreten können, zu entdecken. Wenn Sie den Bericht überprüft haben, können Sie das Datensicherungsprogramm beenden.

Wiederherstellung von Daten bei Windows XP

Gehen Sie im Startmenü auf den Menüpunkt "Alle Programme", dann auf "Zubehör". Es öffnet sich eine neue Schaltfläche, dort wählen Sie "Systemprogramme" aus und anschließend klicken Sie auf "Sicherung".

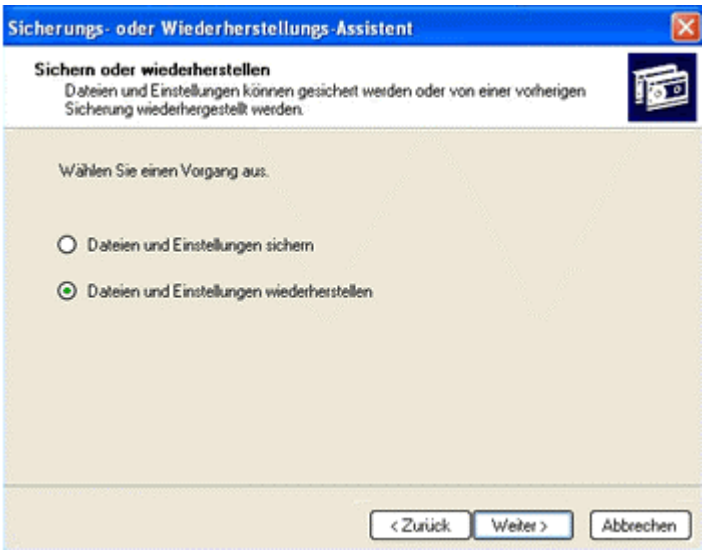


Anschließend sehen Sie den Sicherungs- oder Wiederherstellungs-Assistenten.



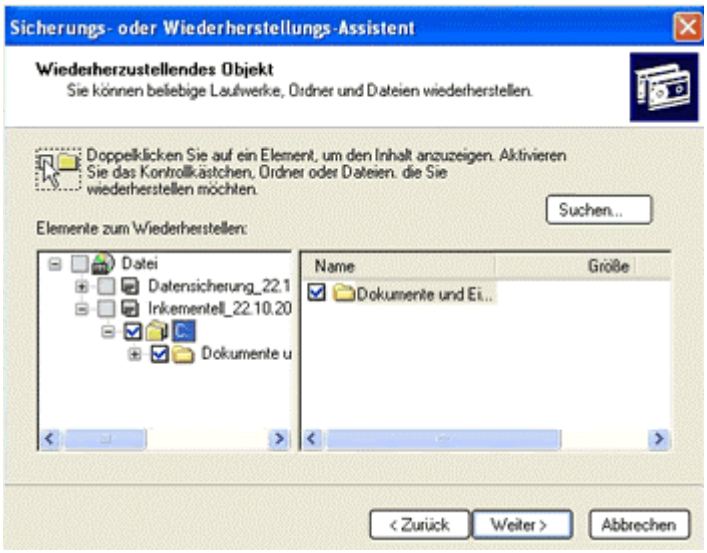
Für normale Benutzer empfiehlt es sich, immer im Assistent-Modus zu starten, deshalb setzen Sie ein Häckchen in diesem Feld und drücken auf "Weiter".

Im nun folgenden Fenster entscheiden Sie sich diesmal für Punkt 2: "Dateien und Einstellungen wiederherstellen".

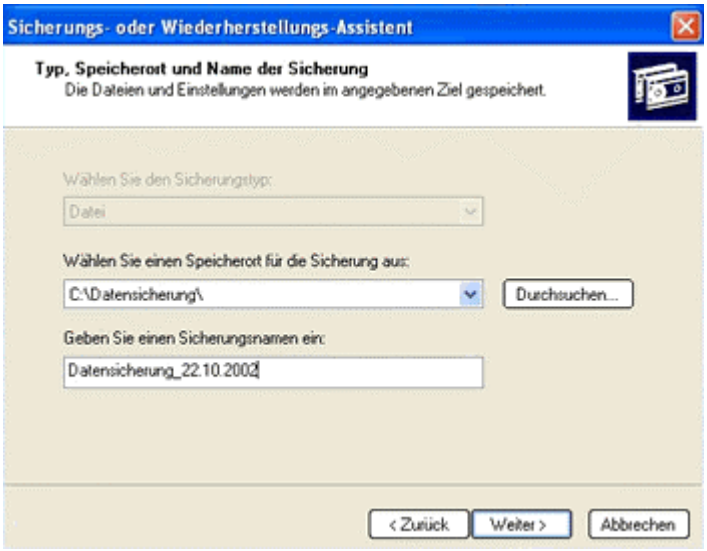


Mit einem Klick auf "Weiter" gelangen Sie zum nächsten Fenster.

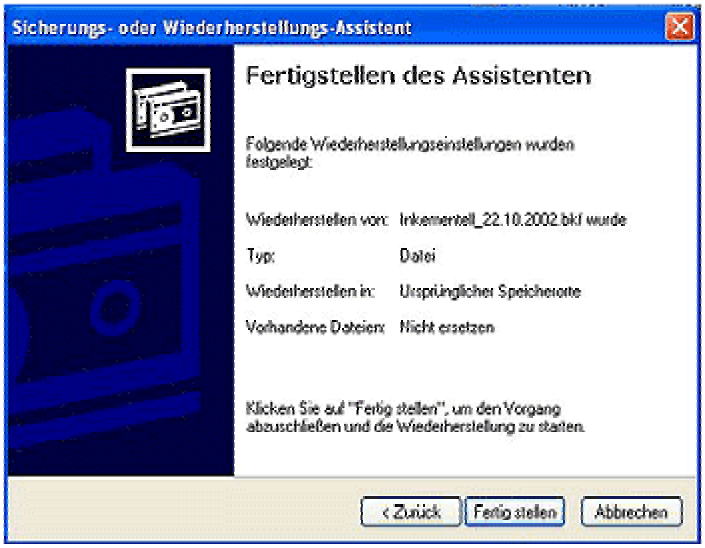
Hier werden Sie gefragt, welche Laufwerke, Ordner oder Dateien wiederhergestellt werden sollen. Sie müssen sich entscheiden, aus welcher Datensicherung die Daten wiederhergestellt werden sollen.



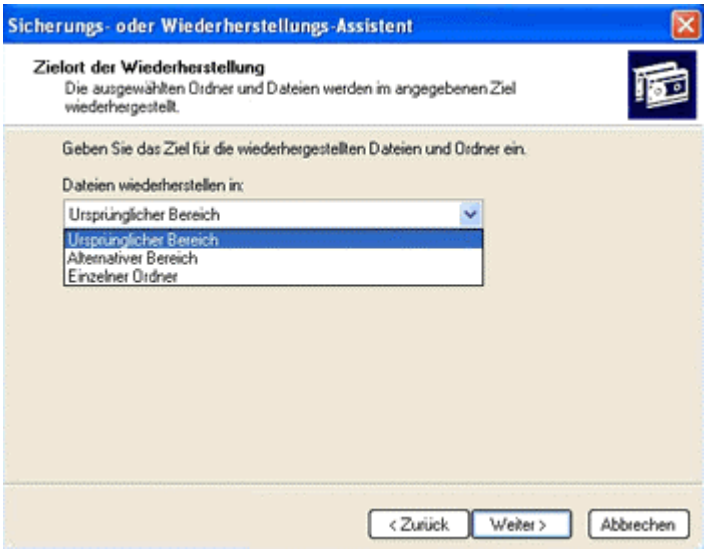
Durch den Klick auf "Weiter" gelangen Sie zum nächsten Fenster.



Wenn Sie Ihre Auswahl mit "Weiter" bestätigt haben, erscheint ein Fenster, in dem Sie alle Ihre Einstellung noch einmal auf einem Blick sehen.

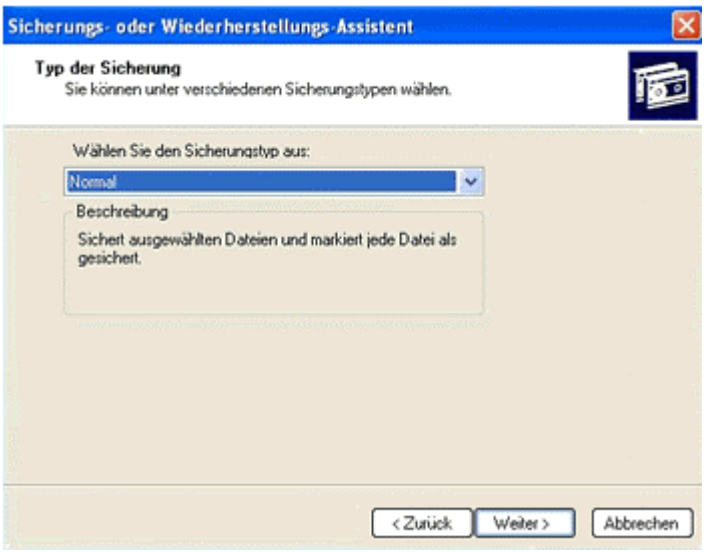


Diese Einstellungen können Sie durch einen Klick auf "Fertig stellen" besiegeln oder durch einen Klick auf "Erweitert..." anpassen. Im Beispiel wird auf "Erweitert" geklickt. Sie gelangen dann zu folgendem Fenster.

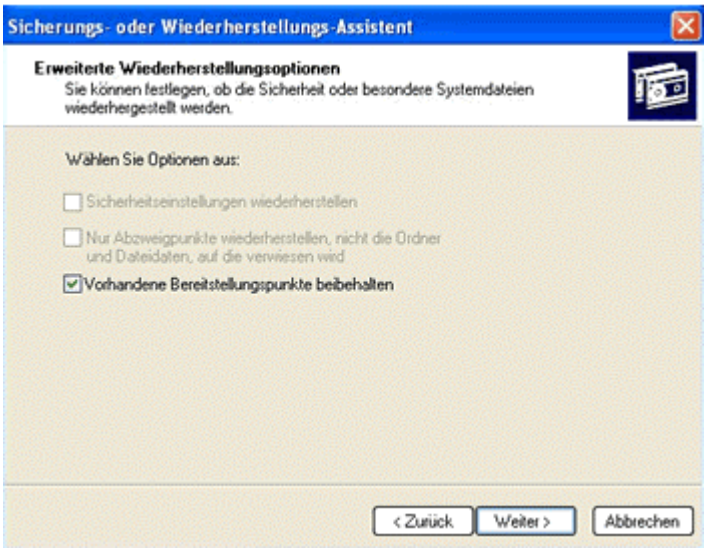


Sie können beispielweise bestimmen, wo die Dateien und Ordner wiederhergestellt werden sollen.

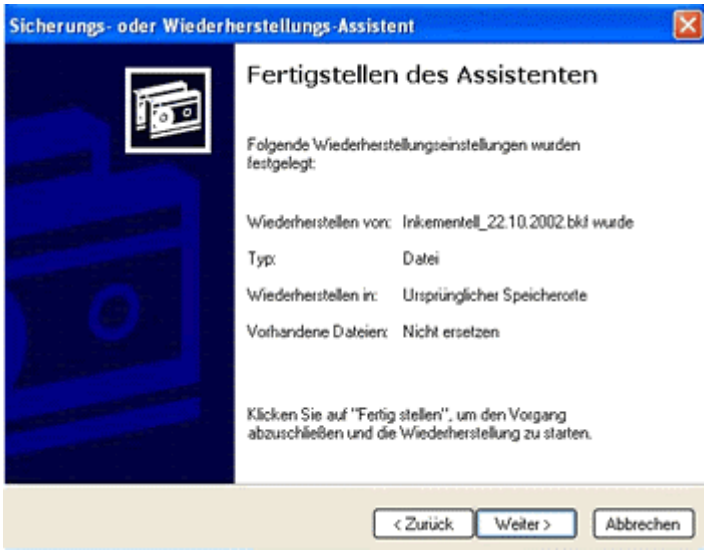
Der Wiederherstellungs-Assistent empfiehlt Ihnen, die vorhandenen Dateien beizubehalten.



Je nachdem welchen Wiederherstellungstyp Sie durchführen und was Sie dadurch für eine Vorauswahl getroffen haben, können Sie hier weitere Optionen auswählen. Für detaillierte Hilfe zu den Optionen können Sie F1 drücken.



Mit einem Klick auf "Weiter" gelangen Sie zum letzten Fenster vor der Wiederherstellung.



In diesem Fenster werden Ihre Einstellungen noch einmal im Überblick gezeigt. Um die Wiederherstellung zu starten klicken Sie auf "Fertig stellen".

Nach Abschluss der Datensicherung erhalten Sie auch hier einen Bericht. Wenn Sie auf "Bericht" klicken, können Sie überprüfen, ob alles reibungslos über die Bühne ging oder ob eventuell Probleme aufgetreten sind. In dem hier gezeigten Fall war alles unproblematisch, da nur die letzte Datensicherung wiederhergestellt wurde.

Ein letzter Tipp: Verlassen Sie sich nicht ausschließlich auf Ihre regelmäßig durchgeführten Datensicherungen. Im Ernstfall ist es hilfreich, wenn Sie bei Gelegenheit mal einen Probelauf durchgeführt und eine Wiederherstellung schon einmal ausprobiert haben.

Quelle: http://www.bsi-fuer-buerger.de/04/

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.

Viren

Virentypen
Verbreitungswege
Infektionsarten
Virenaufbau
Mögliche Schäden durch Computer-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 2002 waren rund 90.000 unterschiedliche Computer-Viren im Umlauf. Jeden Monat entstehen Dutzende 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.

Virentypen

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.

Verbreitungswege

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.

Infektionsarten

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.

Virenaufbau

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.

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"

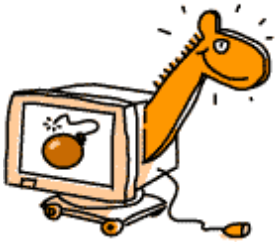
Für Geschäftsbriefe ist dieser Computer damit nicht mehr tauglich. Dieser Virus ist aber noch einer der harmloseren Sorte. Andere können auch sämtliche Kundendaten von Unternehmen löschen. Sind diese Daten nicht vorher gesichert worden, kann das Unternehmen im schlimmsten Fall nicht mehr weiterarbeiten.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

Würmer

Eine Variante von Viren, von denen man in letzter Zeit immer öfter hört, sind so genannte Würmer. Die Infektion erfolgt oftmals über E-Mail. Startet man eine angehängte Datei, wird der Virus aktiviert und verbreitet sich anschließend selbst weiter. Durch Sicherheitslücken in einigen E-Mail-Programmen können sich die Würmer besonders schenll verbreiten. Bei Outlook und Outlook Express von Microsoft ist es sogar möglich, die verseuchten E-Mails ohne Wissen des Benutzers an Personen aus dem Adressbuch zu versenden. Weil die Empfänger den Absender der E-Mail kennen, geraten sie in Versuchung, den Anhang zu öffnen und der Wurm pflanzt sich fort.

Im Gegensatz zu Viren und Trojanischen Pferden **infizieren Würmer jedoch keinen fremden Code**, um sich fortzupflanzen. Sie sind auf die selbstständige Verbreitung in Netzwerken ausgerichtet und stehlen lediglich Rechenzeit. Dadurch können sie aber innerhalb kürzester Zeit Hunderte PCs infizieren und diese lahm legen. Ein bekannter Vertreter von Würmern ist der "Nimda", der im September 2001 die Welt in Aufruhr versetzte.

Trojanische Pferde



Das ursprüngliche Trojanische Pferd bestand aus Holz und war eine Kriegslist der Griechen gegen die Trojaner. Der Legende nach versteckten sich ein paar Griechen im Bau des Pferdes. Sie gelangten so nachts nach Troja, weil die Trojaner das Pferd in die Stadt holten, um es der Göttin Athene zu schenken - jedoch ohne die Gefahr im Innern des Pferdes zu ahnen. Einmal in Troja angekommen, eroberten Griechen alsbald die Stadt.

Die Computerversion des Trojanischen Pferdes funktioniert nach dem selben Prinzip. **Ein scheinbar nützliches Programm hat ein anderes sozusagen im Bauch**, das dann unbemerkt eindringt und sich auf dem PC installiert. So können beispielsweise Passwörter und andere vertrauliche Daten ausgespäht, verändert, gelöscht oder bei der

nächsten Datenübertragung an den Angreifer verschickt werden. **Dieser "Datendiebstahl" bleibt in der Regel unbemerkt**, weil im Gegensatz zum Diebstahl materieller Dinge nichts fehlt. Anders als Computer-Viren können sich Trojanische Pferde jedoch nicht selbständig verbreiten.

Mit der zunehmenden Zahl von Internetnutzern verbreiteten sich auch Trojanische Pferde. Es sind Hunderte von Programmen bekannt, die Zugangsdaten von Anwendern erfassen und über das Internet an den "Interessenten" verschicken können.

Hoaxes (Falschmeldung)

"Hoax" ist eine englische Bezeichnung für "schlechter Scherz". Im Deutschen kennt man auch den Begriff "Zeitungsente". Der Begriff Hoax hat sich im Internet als Bezeichnung für die zahlreichen **falschen Warnungen vor bösartigen Computerprogrammen eingebürgert**. Angeblich können diese Festplatten löschen, Daten ausspionieren oder anderweitig Schaden auf den Rechnern der Betroffenen anrichten. Nicht nur Neulinge im Netz, sondern auch erfahrene Administratoren fallen auf die schlechten Scherze herein, die via elektronischer Post (E-Mail) wie ein Kettenbrief durch das Internet wandern.

Die meisten "Hoaxes" sind nach dem gleichen Schema gestrickt:

- Sie beginnen mit einem Aufhänger, der Seriosität vermitteln soll
- Es folgt die angebliche Aufklärung über die Bedrohung aus dem Netz
- Gefolgt von der Bitte, diese Warnung möglichst allen Bekannten zukommen zu lassen.

Beispiel:

Date: xx 2002 11:09:04 +0200
From: N.N.
Subject: Viruswarnung

Hallo Leute, da ich die Datei auch gefunden habe, schicke ich die Warnung weiter.
siehe unten

Viele Grüße Susi Ahnungslos

Virus!
Du kannst den Virus löschen, indem Du die Anweisungen
befolgst. Er verteilt sich über das Adressbuch über Windows/C:.

Er kann wie folgt entfernt werden:
1. Gehen Sie in Windows unter Extra, Suchen,
Dateien/Ordner
2. Unter dem Namen Fenster schreiben Sie: "jdbgmgr.exe"
3. Im Fenster Suchen gehen Sie auf "(C:)"
4. Klicken Sie nun auf: Suche Starten

5. Der Virus hat einen kleinen Bär als Icon vor dem Namen "jdbgmgr.exe"
AUF KEINEN FALL ÖFFNEN!
6. Klicken Sie ihn mit der rechten Maustaste an und entfernen Sie ihn in den Papierkorb.
7. Gehen Sie auf den Papierkorb und leeren Sie ihn komplett.
Falls Sie den Virus finden, warnen Sie bitte alle Adressen aus Ihrem Adressbuch, auch wenn Sie in der letzten Zeit keine e-mails verschickt haben, damit Sie ebenalls ihre E-mail-Partner warnen können.
Der Virus schläft etwa 14 Tage, bevor er Ihren Computer beschädigt.

Dies nur zur Sicherheit und Information.

Befolgt man diese Anleitung, löscht man keinen Virus, sondern eine (relativ unwichtige) Windows-Systemdatei.

Generell werden nämlich **nie echte Virus-Warnungen auf diese Weise** verschickt! Wenn Sie also angebliche Virenwarnungen erhalten, dann tun sie eines: **Löschen Sie die E-Mail und schicken Sie auf keinen Fall weiter**. Nur bei den Herstellern von Antivirensoftware oder öffentlichen Institutionen (wie das BSI) erhalten Sie wirklich seriöse Informationen über drohende Viren. Auch eine Zusammenstellung mit den im Umlauf befindlichen Hoaxes finden Sie dort.

Der wirtschaftliche Schaden, den Hoaxes oder andere Massenmails anrichten, ist enorm, betrachtet man das ganze global: Eine solche Hoax- E-Mail kann per Schneeball-System an Tausende von Personen über Wochen, Monate oder gar Jahre weitergereicht werden. Jede dieser Personen verbringt mindestens eine Minute teure Arbeits- oder kostbare Freizeit damit, die E-Mail zu lesen und zu löschen. Zusätzlich ensteht jede Menge ungewollter Datenverkehr auf den Backbones des Internet, der wiederum heftige Kosten verursacht, die irgendjemand (also auch Sie als normaler Nutzer) tragen muss. Insgesamt kommt so viel Zeit und Geld zusammen, die verschwendet werden!

Viren-Chronik

Bei all dem Schaden, den Viren, Würmer und Trojanische Pferde anrichten, fragen Sie sich jetzt vielleicht: Wer programmiert eigentlich Computer-Viren? Der Personenkreis reicht vom Schüler, der seinem Freund einen Streich spielen will, über das verkannte Genie, das glaubt, auf diese Weise seine Programmierkunst beweisen zu müssen, bis hin zum Techno-Terroristen, der möglichst viel Schaden anrichten will.

Fest steht jedenfalls, dass es Computer-Viren schon sehr lange gibt. Deshalb hier eine kleine Chronik:

1980 verfasste Jürgen Kraus am Fachbereich Informatik der Uni Dortmund eine Diplomarbeit mit dem Titel "Selbstreproduktion bei Programmen". Darin beschreibt er, dass sich Computerprogramme wie biologische Viren verhalten können: Durch eigenständiges Ausbreiten und Vermehren. Weil Kraus aber nicht auf das Problem der PC-Sicherheit eingeht, wurde die Arbeit nicht veröffentlicht und verschwand im Archiv der Universität.

1984 veröffentlichte der Amerikaner Fred Cohen seine Arbeit "Computer Viruses - Theory and Experiments". Er geht besonders auf Viren als Sicherheitsrisiko ein. Cohens Überlegungen finden daher weltweit Beachtung. Von ihm stammt auch die Definition des Begriffs Computer-Virus: A "computer virus" is a program that can "infect" other programs by modifying them to include a possibly evolved version of itself.

1986 erscheinen Viren zum ersten Mal auf IBM-kompatiblen Personal Computern. Sie waren einfach gebaut und gaben meist zu einer bestimmten Zeit eine Meldung aus. In der Virusbranche hält sich hartnäckig folgende Legende: Die Brüder Basit und Amjad Alvi aus Lahore in Pakistan sollen "Brain", den ersten PC-Virus geschrieben haben, weil sie sich als Inhaber einer Software-Firma über Raubkopierer geärgert haben. Deshalb, so die Legende, schoben sie ihnen einen Virus unter.

1987 legte der "Christmas Tree" (Weihnachtsbaum) das weltweite IBM-Netzwerk lahm. Auch das vom Militär entwickelte dezentrale Netzwerk ARPANET - das Ur-Internet - ist Ziel der Virenattaken. Ende der 80er-Jahre entwickelten Virus-Autoren immer kompliziertere Mechanismen, um die Viren zu tarnen. Dadurch wird die Virus-Suche sehr aufwändig. Die so genannten Tarnkappen-Viren tauchten 1990 das erste Mal auf. Im selben Jahr erschienen Viren-Suchprogramme auf dem Markt, die bereits rund 40 verschiedenen Virenarten erkennen konnten.

1990 schrieb Marc Washburn "1260", den ersten polymorphen Virus. So bezeichnet man Programme, die ihren Quellcode fortlaufend ändern können und daher schwierig zu identifizieren sind.

1991 kam der Boot-Virus "Form". Er war bis dato einer der erfolgreichsten Viren und blieb acht Jahre lang in den Viren-Top-10. Am 18ten jedes Monats wurde er aktiv: Beim Drücken einer beliebigen Taste ertönte ein Klickton. Bei "Windows NT" gab es Probleme mit dem Booten.

1992 sorgte der Virus "Michelangelo" für die erste Viren-Hysterie. Auf der ganzen Welt fürchteten sich PC-Nutzer vor einer Infektion. Der Virus nistete sich in den Boot-Sektor

von Disketten und dem Start-Sektor der Festplatte ein und löschte am 6. März die Festplatte. Aufgrund des Datums 6. März, dem Geburtstag des italienischen Malers und BildhauersMichelangelo, wurde er nach ihm benannt.

1993 gibt es täglich zwei bis drei neu Viren. Aber so richtig neu sind die Viren meist nicht, sie sind Varianten der bisherigen.

1994 wurde der erste Viren-Hoax bekannt.

1995 gerät der erste Makro-Virus "Concept" in Umlauf.

1998 kommt drei Jahre später mit dem "CIH-Virus" der erste Virus, der auch Hardware beschädigen kann: Er löscht nicht nur die Festplatte des befallenen Computers, sondern überschreibt unter Umständen auch das Flash-BIOS. Erst wenn man den beschädigten BIOS-Chip austauscht, kann der infizierte Rechner wieder benutzt werden.

1999 richtete der Makro-Virus "Melissa" große Schäden an - vor allem bei internationalen Firmen - und lässt viele Rechner zusammenbrechen. Als erster Virus öffnet er die Adressbücher von Outlook und Outlook Express und verbreitet sich über Massen-E-Mails.

2000 tauchte dann der "Loveletter" auf. Experten sprechen von sich am schnellsten verbreitenden Virus der Computergeschichte. Mittlerweile sind dutzende Klone entstanden, die mit abweichenden Namen und Endungen versuchen, sich weiter zu verbreiten.

2001 steigt durch zunehmende Zahl der Internetnutzer auch die Anzahl der Computer-Viren. Die Viren verbreiten sich immer schneller. Der Virus "Kournikova" breitet sich aus, "Code Red" befällt binnen weniger Stunden 250.000 Rechner und verursacht einen Schaden von zwei Milliarden US-Dollar. Der Virus "SirCam" sichert sich von Juli bis August den ersten Platz in den Top-10 der Virus-Hitliste. Eine Woche nach den Terroranschlägen in den USA taucht ein Wurm namens "Nimda" auf.

2002 Ein neuer Wurm mit dem Namen "Klez" verwendet bei seiner Verbreitung fast immer gefälschte Absenderadressen. Der richtige Absender befindet sich im Kopfteil der empfangenen Nachricht und kann nur schwer ermittelt werden. Bei der Verbreitung über E-Mail nutzt er eine Sicherheitslücke in Microsoft Outlook und Outlook Express. Dadurch wird der Wurm sofort aktiviert, wenn die E-Mail gelesen wird oder wenn die AutoVorschau aktiviert ist.

Quelle: http://www.bsi-fuer-buerger.de/05/

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 im letzten Jahr im 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.

0190-Dialer

Warum gibt es Dialer?
So funktioniert ein Dialer
Das können Dialer normalerweise nicht
So können Sie sich schützen - Tipps
Daran erkennen Sie einen Dialer
Das können Sie tun, wenn ein Dialer bei Ihnen aktiv war
Schon von 0900-Nummern gehört?

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?

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 (Glossar) ins Internet eingewählt hat. Das böse Erwachen kommt Wochen später mit der Telefonrechnung.

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.

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. Legen Sie die maximale Höhe der Telefonrechnung bei Ihrem Netz-Betreiber fest.

2. Lassen Sie 0190- Nummern sperren.

3. Beantragen Sie einen Einzelverbindungsnachweis. Dieser ist für Sie kostenlos.

4. Richten Sie keinen automatischen Internet-Zugang ein! Speichern Sie Ihr Zugangspasswort nicht ab.

5. Installieren Sie ein Dialer-Schutzprogramm, einen so genannten "0190-Warner (Toolbox)

6. Meiden Sie unbekannte Software, E-Mails oder "kostenlose" Dialer.

7. Deaktivieren Sie AktiveX und andere Aktive Inhalte, über die sich Dialer unbemerkt einnisten können.

8. Schalten Sie Ihr - soweit vorhanden - externes Modem ab.

9. Ziehen Sie bei seltener Internet-Nutzung gegebenenfalls das Kabel aus der Telefondose.

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!

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"

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
     www.denic.de für .de-Domains,
     www.ripe.net für europäische Adressen oder
     www.networksolutions.com für com/.net/.org-Domains
   - Vollständige 0190-Rufnummer ermitteln
2. **Erstatten Sie Strafanzeige bei der Polizei!** (Siehe auch Kapitel: Recht im Internet - Hinweise des BKA)

3. **Erheben Sie Einwände gegen die Telefonrechnung!**

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

Ihre Telefonrechnung werden Sie möglicherweise trotzdem bezahlen müssen. Darauf bestehen die Telekommunikationsunternehmen und die Rechtslage ist hierzu noch nicht eindeutig. Ihre Chancen nicht auf den Kosten sitzen zu bleiben, stehen aber in jedem Fall besser, wenn Sie nachweisen können, dass es sich um einen unseriösen Dialer handelt, der sich ohne Ihr Wissen bei Ihnen eingenistet hat.

Anlage Dialerschutz (Stand: April 2002) von der Verbraucherzentrale NRW, BW, Brandenburg
www.vz-nrw.de/mediabig/2803A.pdf

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)

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.

Hacker

Hacker sind Personen, die **illegal** versuchen, über Datennetze in fremde Computersysteme einzudringen. Sie löschen, verändern oder missbrauchen geschützte Datenbestände oder Programme. Manchmal entstehen durch solche Eingriffe materielle **Schäden in Millionenhöhe**. Allerdings helfen manche Hacker auch die Sicherheit des Internets zu verbessern, denn sie machen auf Schwachstellen oder Sicherheitsdefizite in Computernetzwerken aufmerksam.

Hacker, die im Auftrag von Firmen versuchen, Sicherheitslücken aufzuspüren, werden auch als "Penetrationstester" bezeichnet. Sie handeln legal, weil sie beauftragt werden und sich an Vorgaben halten, was mit den gewonnenen Erkenntnissen passiert. Außerdem sind sie abgesichert, wenn durch die Hackversuche Schäden entstehen.

Denial-of-Service-Attacken

Denial of Service - oder kurz DoS - bedeutet soviel wie etwas unzugänglich machen oder **außer Betrieb setzen**. Technisch passiert dabei folgendes: Bei DoS-Attacken wird ein Server gezielt mit so vielen Anfragen bombardiert, dass das System die Aufgaben nicht mehr bewältigen kann und im schlimmsten Fall zusammenbricht. Auf diese Art wurden schon bekannte Web-Server wie zum Beispiel Amazon, Yahoo, eBay, mit bis zur vierfachen Menge des normalen Datenverkehrs massiv attackiert und für eine bestimmte Zeit für normale Anfragen außer Gefecht gesetzt.

Die Programme, die für DoS-Angriffe genutzt werden, sind mittlerweile sehr ausgefeilt und die Angreifer sind nur schwer zu ermitteln, weil sich der Weg der Daten verschleiern lässt. Möglich sind einige der Attacken durch Bugs und Schwachstellen von Programmen, Betriebssystemen oder Fehlimplementierungen von Protokollen.

Andere Angriffe überlasten schlicht das ganze System mit zu vielen Anfragen.

Es existieren daher auch **verschiedene Formen einer DoS-Attacke:**
• Syn Flooding:
Zu Beginn eines Verbindungsaufbaus wird in TCP/IP basierten Netzen ein sogenannter Handshake durchgeführt. Dabei werden so genannte SYN - und ACK -Datenpakete

ausgetauscht. Bei einem SYN-Flooding-Angriff werden an ein Computersystem sogenannte SYN-Pakete geschickt, die anstatt der eigenen Absenderadresse eine gefälschte im Internet erreichbare IP-Adresse tragen. Das angegriffene Computersystem versucht nun auf die SYN-Pakete mit SYN-ACK-Paketen zu antworten. Aber weil die Absenderadresse des ersten Paketes gefälscht war, kann das System unter dieser Adresse nicht den Computer erreichen, der eine Verbindung zu ihm aufbauen wollte. Erst nach einer gewissen Zeit werden die Verbindungsversuche von Seiten des angegriffenen Systems aufgegeben. Wenn nun eine große Anzahl von gefälschten SYN-Paketen eintrifft, verbraucht der angegriffene Rechner alle seine Verbindungskäpazitäten auf das hoffnungslose Versenden von SYN-ACK-Paketen und ist somit von anderen Systemen aus nicht mehr zu erreichen.

• Ping Flooding:
Ping ist ein Programm, das prüft, ob andere Rechner im Netz überhaupt erreichbar sind. Beim Ping Flooding bombardiert der Angreifer den Zielrechner mit einer gewaltigen Menge von so genannten Pings. Der ist nur noch damit beschäftigt die Pings zu beantworten (mit dem so genannten Pong) und je nach Art und Größe der Pings pro Sekunde, kann dies bei Rechnern mit älteren Betriebssystemen innerhalb kürzester Zeit zu einem Systemabsturz führen. In jedem Fall führt Ping Flooding zu einer wesentlichen Beeinträchtigung des angegriffenen Rechners und vor allem des Netzwerkes, in dem sich dieser Rechner befindet. Neben dem Systemausfall entstehen außerdem hohe Kosten, wenn die Netzwerkverbindung nicht nach Zeit sondern nach erzeugter Datenmenge abgerechnet wird.

• Mailbombing:
Dabei wird entweder eine enorm große Nachricht in Form einer E-Mail an die Zieladresse geschickt oder die Zieladresse wird mit Tausenden von Nachrichten bombardiert. Das führt zum Verstopfen des Mail-Accounts. Im schlimmsten Fall wird der Mail-Server langsamer oder bricht total zusammen. Solche Mail-Bombing-Angriffe können ohne größere Probleme durch im Internet erhältliche Programme durchgeführt werden.

Verteilte Denial-of-Service-Attacken
Seit einiger Zeit gibt es auch vermehrt so genannte "verteilte DoS-Attacken". Dabei kommt anstelle von einzelnen Systemen eine Vielzahl von unterschiedlichen Systemen in einem großflächig koordinierten Angriff zum Einsatz. Durch die hohe Anzahl der gleichzeitig angreifenden Rechner sind die Angriffe besonders wirksam. Im Englischen wird diese Art Angriff als Distributed Denial of Service (DDoS)-Angriff bezeichnet. Eine DDoS-Attacke ist daran zu erkennen, dass sie deutlich mehr Netzressourcen als der normale Verkehr beansprucht.

In der Praxis können Sie sich das so vorstellen: Ein Hacker verteilt seine Angriffsprogramme auf mehreren hundert bis tausend ungeschützten Rechnern. Besonders beliebte "Opfer" sind Server in Universitätsnetzen, denn sie laufen meist rund um die Uhr im Gegensatz zu Ihrem Heim-PC. Diese Rechner werden zum Angriffswerkzeug, denn auf Kommando des Hackers bombardieren sie ein bestimmtes Ziel mit gefälschten Anfragen, zum Beispiel einen Web-Server. Der ist dann außer Gefecht gesetzt. Sich vor solchen Angriffen zu schützen ist deshalb schwer, weil der

Zielrechner die Daten erst erhalten muss, um sie zu analysieren. Doch dann ist es bereits zu spät. Die Hacker selbst lassen sich nur schwierig aufspüren, da sie in den meisten Fällen mit gefälschten IP-Quelladressen arbeiten. Deshalb muss verhindert werden, dass DDos-Programme wie "Stacheldraht" oder "TFN 2K" überhaupt eingeschleust werden.

Spyware

Nicht nur Viren und Würmer können Ihnen das Leben schwer machen. Auch die **Schnüffel-Software** im Web wird zur Plage: Hunderte Spione kennen Ihre Hobbys, oder sammeln Ihre Bookmarks. Ihr Recht auf Diskretion und Datenschutz im Internet wird durch kleine, oft unbemerkt installierte Hintergrundanwendungen, Plug-Ins und Dateien gefährdet. Solche Spionageprogramme werden Spyware genannt. Vor allem bei der **Installation von Shareware- oder Freewareprogrammen fangen Sie sich die Spione ein**.

Oft passiert das sogar freiwillig. Wenn Sie eine Software auf Ihrem PC installieren und sich dafür dann registrieren lassen, erklären Sie sich schon mit einem Doppelklick auf das so genannte "Privacy Statement" mit der Spionage einverstanden. Ihr Browser und die bisher besuchten Webseiten werden dann dazu benutzt, um zum Beispiel zu erkennen, welche Werbeanzeigen Ihnen auf den jeweiligen Seiten gezeigt werden sollen. Das Programm untersucht also, welche Webseiten Sie besuchen, was Sie herunterladen, welchen Namen und welche E-Mail-Adresse Sie haben, wo Sie wohnen und welche Daten Sie während der Registrierung freiwillig eingeben. Interesse an diesen Daten haben natürlich die Programmhersteller und spezielle Werbefirmen.

Es gibt jedoch auch verschiedene Programme, die sich mit der Übermittlung von persönlichen Daten im Rahmen der Registrierung nicht begnügen. Diese erzeugen eine rechnerspezifische Identifikationsnummer, die mit hoher Wahrscheinlichkeit einmalig ist und die Möglichkeit bietet, den Rechner - und damit den Benutzer - zu identifizieren. Darüber hinaus gibt es aber noch weitere Varianten, wie bestimmte Programme während des Betriebs nicht näher spezifizierte Daten an den Hersteller übermitteln.

Schützen können Sie sich vor dieser ungewollten Spionage, indem Sie eine **Firewall auf Ihrem Computer einrichten**. Leider gehen Sie damit aber nicht immer auf Nummer sicher, weil sich die kleinen Spione in vielen Fällen an der Firewall vorbeischleusen. Sie können deshalb auch eine Anti-Spy-Software installieren. Damit lassen sich die Spione aufspüren und auch löschen. Ein solches Programm finden Sie übrigens auch in unserer Toolbox.

SPAM

Der Name "Spam" ist dem Dosenfleisch SPAM (**S**piced **P**orc and **H**am) der amerikanischen Firma Hormel Foods entliehen (deutsch: Frühstücksfleisch), den es seit 1937 gibt. Im Internetzeitalter ist er zum **Synonym für Massen-E-Mails** geworden.

Wie der Schinken zur Massen-E-Mail wurde, darüber gibt es viele Geschichten. Hormel Foods selbst sagt, es beruhe auf einem Sketch der Comedy-Gruppe "Monty Python". Darin kam der Begriff über 120mal innerhalb weniger Minuten vor und übertönte jede andere Konversation. Und tatsächlich liegt die Analogie zur Massen-E-Mail damit auf der Hand.

Als Spam, Spamming oder Junk Mail (Müllpost) bezeichnet man im Internet:

- Massenversand nichtangeforderter Werbe- E-Mails
- Werbebeiträge in Newsgroups, die nichts mit dem Thema der Newsgroup zu tun haben.
- Kettenbriefe

Müll und Wurfsendungen in elektronischer Form, die oft kommerzieller Art sind, werden auch **UCE** genannt ("Unsolicited Commercial E-Mails), was soviel heißt wie "unaufgeforderte Werbe-E-Mails".

Um E-Mails in millionenfacher Menge versenden zu können, benötigen die Spammer Adressen. Diese sind bei Adresshändlern zu bekommen. Oft führen kommerzielle Spammer aber auch Datenbanken mit Millionen von Adressen. Durch das gezielte - mit einem Programm automatisierte - Absuchen von Newsgroups, Homepages oder E-Mailverzeichnissen, aber auch durch Durchprobieren gängiger Adressen (info@... usw.) sind die Adressen schnell erhältlich. Aufgrund der großen Menge spielt es dann auch keine Rolle, wenn viele Adressen ungültig sind. Fast alle Kosten - oder Müllgebühren - müssen Sie als Empfänger und die Provider bezahlen: für die angefallene Downloadzeit und den benötigten Speicherplatz. Der Versand erfolgt meist vollautomatisch über spezielle Programme. Der Spammer muss nur das Programm starten und kann dann einer anderen Tätigkeit nachgehen, während sein Programm Hunderttausende von Leuten belästigt.

Weil Massen-E-Mails für den Spammer relativ kostengünstig sind, lohnt sich das Geschäft bereits, wenn auf fünf Millionen Spams fünf Personen ein Produkt kaufen. Jeder, der solche Spam-Mails erhält, wird merken, dass damit hauptsächlich für Dinge geworben wird, für die es sich nicht lohnt, in andere Werbemittel zu investieren. Entweder ist das beworbene Produkt praktisch wertlos oder aber sogar illegal.

Nach deutschem Recht ist es verboten, Personen unaufgefordert Werbung per E-Mail zuzusenden. Spam ist aber weit mehr als nur ein lästiges Übel: Jedes Jahr entstehen **Kosten in Milliardenhöhe** durch die Übertragungskosten für den Versand, den Zeitverlust für das Lesen, Löschen oder Beantworten dieser elektronischen Belästigungen.

Ärgerlich wird es vor allem dann, wenn Ihre Mailbox zugestopft ist und reguläre Post an Sie aufgrund der Größenbeschränkung Ihrer Mailbox abgewiesen wird. Durch übermäßige Nutzung können Server mitunter sogar abstürzen, was massive Verzögerungen und gravierende Schäden zur Folge hat.

Wie Sie sich schützen können - Tipps

• Behandeln Sie Ihre E-Mail-Adresse fast wie eine Geheimnummer
Tragen Sie Ihre Mailadresse nicht überall in Web-Formulare ein. Ihre Haupt-E-Mail-Adresse sollten Sie nur an Personen weitergeben, die Sie persönlich kennen. Genauso sollten Sie auch mit den Adressen Ihrer Freunde und Bekannten verfahren. Zum Beispiel bieten viele Nachrichtenseiten die Option, Artikel oder Nachrichten mit einem Klick an einen Freund zu senden. Wenn Ihnen der Anbieters unseriös erscheint, tragen Sie die Mailadresse Ihres Bekannten nicht in das entsprechende Feld ein. Investieren Sie stattdessen lieber eine Minute mehr Zeit und schicken Sie Ihrem Freund den Link direkt über Ihr Mailprogramm zu.

• Speichern Sie auf Ihrer Homepage Ihre E-Mail-Adresse als Bild-Datei ab
Nachdem die Spammer die HTML-Seiten im Internet nach E-Mail-Adressen (erkennbar am @-Zeichen) durchforsten, speichern Sie einfach Ihre E-Mail-Adresse als Bild-Datei (z.B. GIF) ab. Damit läuft das automatische Sammeln ins Leere.

• Legen Sie sich ein zweites Postfach zu
Auf vielen Internetseiten müssen Sie sich mit Ihrer E-Mail-Adresse registrieren, um bestimmte Dienste in Anspruch nehmen zu können. Daran führt oft kein Weg vorbei. Damit Sie nicht Ihre Haupt-E-Mail-Adresse preisgeben müssen, legen Sie sich für diesen Fall eine zweite E-Mail-Adresse zu, die Sie bei vielen Providern kostenlos erhalten.

• Antworten Sie nicht auf Werbe-E-Mails
Oft enthalten solche Mails am Anfang oder Ende eine Anmerkung nach diesem Muster: "Klicken Sie hier, wenn Sie keine weiteren Mails mehr von uns erhalten möchten" oder "Antworten Sie mit dem Betreff 'Remove', um von der Verteilerliste gelöscht zu werden". Das sollten Sie tunlichst vermeiden, denn dadurch zeigen Sie dem Absender, dass Sie das Postfach regelmäßig nutzen. Das macht Ihre Adresse für den Weiterverkauf noch wertvoller und Sie riskieren dadurch möglicherweise in Zukunft noch mehr Reklamepost zu bekommen. Natürlich gibt es auch Ausnahmen. Bei Newslettern, die Sie bestellt haben, können Sie sich auch ohne weiteres wieder von der Liste entfernen lassen.

• Schalten Sie den Spam-Schutz Ihres E-Mail-Anbieters ein
Kostenlose Maildienste sind ein beliebtes Ziel von Werbeversendern. Auch wenn Sie Ihre neue Adresse an niemanden weitergegeben haben, kann es sein, dass Sie schon innerhalb von kürzester Zeit mit unerwünschten Nachrichten belästigt werden. Abhilfe schafft hier der Spam-Schutz. Bei Hotmail heißt dieser Dienst zum Beispiel "Junk-Mail-Filter", bei GMX müssen Sie unter Optionen "AntiSpam" aktivieren.

• Richten Sie Filter in Ihrem Mail-Programm ein
Wenn Sie immer vom selben Absender durch Werbemails belästigt werden, ist es ziemlich einfach, diese Mails automatisch aussortieren zu lassen. Dazu müssen Sie in Ihrem Mail-Programm einen entsprechenden Filter setzen. Bei Outlook Express klicken Sie beispielsweise auf "Extras, Regeln, E-Mail" und definieren dann die entsprechenden Bedingungen. Auch bei den großen Freemail-Diensten wie GMX, Web.de, Freemail oder Hotmail gibt es derartige Filterregeln. Die unerwünschten Mails werden dann

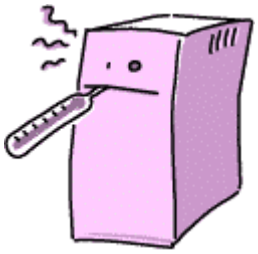
schon auf dem Server gelöscht oder in einen anderen Ordner verschoben.

• **Fallen Sie nicht auf falsche Betreffzeilen herein**
Bevor Sie Mails mit Betreffzeilen wie "Re: Ihre Anmeldung", "Will Dich wiedersehen" oder "Sie haben gewonnen!" öffnen, schauen Sie besser erst einmal auf den Absender. Oft sollen die Betreffzeilen nämlich nur Aufmerksamkeit erwecken und halten nicht, was sie versprechen.

• **Tragen Sie sich in die Robinsonliste ein**
Es gibt Listen für Postanschriften und auch für virtuelle Werbung, in die man sich eintragen kann, wenn man keine unverlangte Werbung wünscht. Eine Liste ist die Robinsonliste, (www.robinsonliste.de) des Interessenverband Deutsches Internet e.V. . Registrierte Unternehmen haben Zugriff auf die Liste und können die eingetragenen Adressen aus ihrer Datenbank löschen.

Quelle: http://www.bsi-fuer-buerger.de/06/

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?

Daran erkennen Sie, ob Ihr PC infiziert ist

Computer benehmen sich oft anders, als Sie es gerne hätten. Wenn aber ...

- Ihr Betriebssystem auf bestimmte Laufwerke oder Datenträger nicht zugreifen kann
- Ihr Rechner nicht mehr hochfährt
- die Icons anders als sonst aussehen
- sich Dateien nicht mehr ändern oder abspeichern lassen
- oder der Zugriff auf Dateien länger als normal dauert

... kann es sein, dass sich Ihr PC einen Virus eingefangen hat. Aber nicht immer ist ein Virus die Ursache. Es kann sich auch um einen Hardware- oder sonstigen Software-Fehler handeln.

Vorbeugen ist das A und O

Wie Sie bereits wissen, ist ein Virus für Ihren PC so ähnlich wie für Sie eine Grippe. Nur, dass Sie Ihren Rechner nicht zum Arzt bringen müssen. Wichtiger ist vielmehr, ihn vor der Infektion zu schützen. Das können Sie tun, indem Sie ein **Anti-Viren-Programm** oder **Virenscanner** installieren.

Früher mussten die Benutzer das Viren-Schutzprogramm in regelmäßigen Zeitabständen starten und dann wurde die ganze Festplatte, einzelne Laufwerke, Disketten oder CD-ROMs überprüft. Heute ist es viel einfacher. Wenn die Auto-Protect-Funktion eingeschalten ist, überprüft das Programm Ihren Rechner nach jedem Systemstart automatisch im Hintergrund. Sie erkennen das am Icon in der Task-Leiste. Wird ein Virus gefunden oder hat der Scanner etwas Verdächtiges bemerkt, erhalten Sie eine Nachricht in einem Mitteilungsfenster.

Das Programm kann natürlich nur vor den Viren warnen, die es kennt. Und da täglich mehr als zwanzig neue Viren dazu kommen, ist das Programm nicht lange auf den aktuellen Stand und damit wirkungsvoll. Deshalb müssen Sie die Software **regelmäßig aktualisieren** (updaten); das erste Mal am besten direkt nach der Installation. Manchmal machen die Programme das auch von allein; das kommt ganz auf den Hersteller an. Die Updates bieten die meisten Hersteller im Internet an.

10 Tipps zum Virenschutz

Um das Risiko einer Infektion und der Ausbreitung des Computervirus so gering wie möglich zu halten, sollten Sie sich ständig über die Art der Gefahren informieren, einige Vorsichtsmaßregeln beachten, für den Notfall Vorsorge zu treffen und sich durch wirksame Mittel vor einer Neuinfektion weitmöglichst zu schützen. Die meisten Computer-Viren sind zum Glück nur lästig und vernichten keine Daten und Programme absichtlich.

Deshalb:

1. Sichern Sie regelmäßig Ihre Daten

2. Bewahren Sie die Sicherheitskopien sorgfältig auf.

3. Versehen Sie alle Datenträger, auf denen nicht geschrieben werden muss, mit Schreibschutz.

4. Verwenden Sie aktuelle Anti-Viren-Software und aktualisieren Sie diese regelmäßig.

5. Überprüfen Sie Datenträger, die Sie verwenden, mit dem Anti-Viren-Programm.

6. Überprüfen Sie auch vorinstallierte Neugeräte und Geräte, die gewartet wurden.

7. Erstellen Sie einen Notfall-Datenträger (Diskette oder CD-ROM).

8. Um den besten Schutz vor Boot-Viren zu erhalten, sollten Sie die Boot-Reihenfolge im CMOS-RAM von "A:, C:" auf "C:, A:" ändern.

9. Richten Sie mehrere Partitionen auf dem Rechner ein.

10. Schützen Sie Ihren Computer und alle Datenträger vor fremder Benutzung.

Infektionsbeseitigung

10 Dinge, die Sie bei einer Infektion tun sollten:

1. Bei Verdacht auf Virus-Befall sollten Sie die Arbeit schnell, aber wie gewohnt beenden. Vor allem gilt: Keine Panik!

2. Schalten Sie den Computer aus.

3. Wenn Sie kein Experte sind, holen Sie sich lieber den Rat eines solchen ein. Manchmal ist zur Virenbeseitigung besondere Fachkenntnis erforderlich, da Viren sich in ihrer Arbeits- und Wirkungsweise stark unterscheiden können.

4. Legen Sie eine virenfreie, schreibgeschützte System- bzw. Boot-Diskette in Laufwerk A: ein und booten Sie den Rechner von dieser Diskette. Normalerweise ist der Rechner so voreingestellt, dass er vom Laufwerk A: aus startet. Wenn Sie die Boot-Reihenfolge jedoch geändert haben (siehe Infektionsvorbeugung), müssen Sie sie wieder auf "A:" ändern.

5. Überprüfen Sie den PC mit einem aktuellen Viren-Schutzprogramm. Dadurch können Sie feststellen, ob tatsächlich ein Computer-Virus aufgetreten ist und um welchen es sich handelt.

6. Sichern Sie Ihre Daten, falls noch nicht geschehen.

7. Entfernen Sie den Virus abhängig vom jeweiligen Virustyp. In der Regel macht Ihr Anti-Viren-Programm das automatisch. Sollte das nicht klappen, so können vom Hersteller der Anti-Viren-Programme mitgelieferte Virendatenbanken Hilfestellungen geben. Darin sind die Funktionsweise und die Behebung oftmals detailliert beschrieben.

8. Lassen Sie die Festplatte und alle anderen Datenträger noch einmal überprüfen, um sicherzugehen, dass der Virus auch wirklich komplett entfernt wurde. Stellen Sie die Boot-Reihenfolge des Rechners anschließend wieder auf "C:, A:".

9. Sollte der Computer-Virus Daten gelöscht oder verändert haben, versuchen Sie, die Daten aus den Datensicherungen und die Programme aus den Sicherungskopien der Programme zu rekonstruieren.

10. Versuchen Sie abschließend die Ursache der Vireninfektion festzustellen. Ist die Quelle auf Original-Datenträger zurückzuführen, dann sollte der Hersteller und das BSI informiert werden (Virusmeldebogen). War die Ursache eine Datei oder E-Mail, dann benachrichtigen Sie den Ersteller oder Absender der Datei. Wenn Sie Daten von einem infizierten Rechner verschickt haben, dann warnen Sie auch die Empfänger Ihrer Daten.

Technische Schutzmaßnahmen

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.

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.

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 als Link in der Toolbox.

Quelle: http://www.bsi-fuer-buerger.de/07/

Datenverschlüsselung

Haben Sie sich schon einmal Gedanken darüber gemacht, ob Sie bei Ihren **Telefongesprächen, E-Mails oder besuchten Internetseiten ausspioniert werden**? So unwahrscheinlich ist das nicht. Allerdings ist es auch nicht unmöglich, sich davor zu schützen. Eine Möglichkeit ist, die **Nachrichten zu verschlüsseln**. Da gibt es **symmetrische** und **asymmetrische** Verfahren, **digitale Signaturen** und die **PKI**. Was das alles ist und wie es funktioniert, erfahren Sie auf den folgenden Seiten.

Warum wird überhaupt verschlüsselt?

Daten werden verschlüsselt, um sie zu schützen. Die Verschlüsselung im Internet dient **drei Zielen**:

- Schutz der Vertraulichkeit: Die Nachricht darf nur für den lesbar sein, für den sie bestimmt ist.
- Schutz der Authentizität: Die Echtheit des Absenders soll gewahrt sein. Ist der Absender wirklich die Person, die als Absender angeben wird?
- Schutz der Integrität: Die Nachricht darf auf dem Weg vom Absender zum Empfänger nicht verändert werden.

Welche Verfahren gibt es?

Die Verschlüsselungsverfahren lassen sich danach unterscheiden, wie ein Text verschlüsselt und wieder entschlüsselt werden kann.

1. Symmetrische Verschlüsselung
2. Asymmetrische Verschlüsselung
3. PKI und Digitale Signatur

1. Symmetrische Verschlüsselung:

Stellen Sie sich vor, Sie wären ein römischer Feldherr und hätten ziemlichen Ärger mit den Germanen. Um diesen eine gehörige Lektion zu erteilen, wollen Sie Ihren Truppen einen geheimen Angriffsbefehl per Boten zukommen lassen. Weil Sie aber befürchten, dass der Bote unterwegs in Feindeshand gerät, chiffrieren Sie die Nachricht.

Der Text sieht dann so aus:

"DQJULIILPPRUJHQJUDXHQ"

Tatsächlich fangen die Germanen den Boten und versuchen nun eifrig, den Inhalt zu

entziffern. Nach ein wenig Knobeln erhalten Sie den Text in Klarschrift. Versuchen Sie es doch auch einmal!

Jeder Buchstabe wurde durch seinen dritten rechten Nachbarn im Alphabet ersetzt.

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

Der verschlüsselte Text heißt in Klarschrift also: "Angriff im Morgengrauen".

Dieses Verfahren wurde damals tatsächlich von den Römern angewandt. Benannt ist es nach seinem Erfinder Caesar. So richtig schwierig ist es aber nicht, oder?

Es gibt aber auch andere Mechanismen um Nachrichten so zu chiffrieren. Die können nur sehr schwer oder überhaupt nicht geknackt werden. Das glauben Sie nicht? Versuchen Sie jetzt einmal diese Botschaft aufzudecken!

"XZKYDXOWFVCUCTFSJRJQLPOODNBMKLDKOJXIRHBGKF"

Die Verfahrensregel lautet hier: Jeden Buchstaben durch seinen dritten linken Nachbarn im Alphabet ersetzen und dazwischen jeweils einen Buchstaben zusätzlich als "Blender" einfügen, wobei mit Z beginnend absteigend das Alphabet durchgegangen wird. Das war schon knifflig, und man könnte sich noch viel schwierigere Verfahren ausdenken. Die Botschaft war übrigens die gleiche.

In einem Computer funktioniert das ganze auch, allerdings versteht dieser **nur Nullen und Einsen**. Anstelle des Textes tritt nun eine Folge der beiden Zahlen. Diese könnte etwa so aussehen: 010101001011001001

Um die Zahlenfolge zu chiffrieren, kann man eine Rechenregeln anwenden, wie z.B. eine Additionsregel, die so heißen kann: 0+0=0; 1+0=1; 0+1=1 und 1+1=0. Anstelle von Buchstaben werden hier jetzt Zahlen vertauscht. Allerdings haben wir jetzt zwar eine Zahlenreihe und ein Rechenverfahren, aber mit was soll denn bitteschön addiert werden?
Sie ahnen es vielleicht bereits: Mit einem Schlüssel, der selbst wieder aus einer Reihe von Nullen und Einsen besteht. Nehmen wir einmal an, der sieht so aus:

001101000100010011

Also addieren wir diese beiden Zahlenfolgen einmal miteinander:

```
      0101010010110010001 Nachricht
+     0011010001000100011 Schlüssel
-------------------------
=     0110000011110110100 Chiffrat
```

Sie sehen, der Schlüssel ist genauso lang wie die Originalnachricht. Es gibt also sehr viele Möglichkeiten, wie dieser aussieht. Je länger der Schlüssel ist, desto mehr

Variationen gibt es, und um so schwieriger ist es, die geheimen Nachrichten zu dechiffrieren.

Bei einem solchen schlüsselabhängigen Verfahren kann übrigens die Rechenregel jedem bekannt sein, solange nur der Schlüssel geheim bleibt.

Um das Chiffrat wieder in die Ursprungsnachricht zurückzuverwandeln, müssen Sie entweder mit dem Schlüssel subtrahieren oder die Addition einfach noch einmal durchführen.

Sender und Empfänger müssen deshalb über den gleichen Schlüssel verfügen. Schwierig ist dabei, den Schlüssel so auszutauschen, ohne dass ihn ein unbefugter Dritter dabei ausspionieren kann.

Ein anderes Problem der symmetrischen Verschlüsselung tritt auf, wenn sehr viele Leute miteinander kommunizieren wollen. Nehmen wir an, dass 12 Leute verschlüsselt Botschaften austauschen möchten. Weil aber manchmal zwei Leute Geheimnisse untereinander haben, von denen niemand sonst erfahren soll, wollen sie verhindern, dass die jeweils übrigen 10 mitlesen können. Wie viele Schlüssel werden hier also insgesamt benötigt?

Der erste benötigt zunächst 11 Schlüssel. Für sich selbst braucht er zwar keinen, aber für jeden anderen jeweils einen. Der zweite benötigt zwar auch 11 Schlüssel, aber einer davon wurde schon bei dem ersten mitgerechnet. Rechnet man so weiter ergibt sich: 11 + 10 + 9 + 8 + 7 + 6 + 5 + 4 + 3 + 2 + 1 = 66. Bei 50 Personen sind es übrigens 1225, bei 1000 Leuten sogar fast 500.000 verschiedene Schlüssel. Nicht auszudenken, wenn das alle Leute so machen wollen!

Diese beiden Probleme der symmetrischen Verschlüsselung werden mit so genannten asymmetrischen Verfahren gelöst.

2. Asymmetrische Verschlüsselung:

Bei der asymmetrischen Verschlüsselung **gibt es immer zwei sich ergänzende Schlüssel**. Ein Schlüssel - der **Public Key** - für das Verschlüsseln einer Nachricht, ein anderer - der **Private Key** - für das Entschlüsseln. Beide Schlüssel zusammen bilden ein Schlüsselpaar.

Das Besondere an der Sache ist, dass aus dem einem Schlüssel der dazugehörige zweite Schlüssel nicht so leicht erraten oder berechnet werden kann. Dadurch kann man einen Schlüssel des Schlüsselpaares für jedermann öffentlich zugänglich machen. Daher auch die Bezeichnung Public Key.

Stellen Sie sich am besten einen Tresor mit Schnappschloss vor. Sie können etwas einschließen, weil der Tresor sich automatisch schließt, wenn die Tür ins Schloss fällt. Zum Öffnen benötigen Sie allerdings einen Schlüssel. Wie bei dem Tresor kann also jeder mit dem Public Key etwas einschließen. Weil aber nur der Empfänger über den geheimen, den Private Key verfügt, kann nur er die Nachricht entziffern oder etwas aus dem Tresor holen.

Die asymmetrische Verschlüsselung beruht auf mathematischen Verfahren, die in einer Richtung einfach aber in der anderen Richtung schwierig durchzuführen sind. Multiplizieren ist so ein Beispiel:

Jeder kann einfach zwei Zahlen multiplizieren, zum Beispiel:
3 121 163 * 4 811 953 = 15 018 889 661 339
Zahlen in Faktoren zu zerlegen, ist dagegen sehr mühselig: Hat man erst einmal das Produkt, ist es sehr schwierig herauszufinden, aus welchen Faktoren dieses ursprünglich gebildet wurde. Versuchen Sie doch einmal (wenn Sie viel, viel Zeit haben) herauszufinden, aus welchen Faktoren die Zahl 11 099 399 206 043 besteht.

Das Problem mit dem Schlüsselaustausch ist daher elegant gelöst: Der öffentliche Teil kann jedem zugänglich gemacht werden, ohne dass die Sicherheit darunter leiden würde. Man benötigt ja immer noch den geheimen Schlüssel. Ein weiterer Vorteil des Verfahrens ist, dass sehr viel weniger Schlüssel benötigt werden als beim symmetrischen Verfahren. Denn jeder benötigt ja nur ein Schlüsselpaar.

Aber auch asymmetrische Verschlüsselungsverfahren haben **Schattenseiten**:

- Erstens sind asymmetrische Verfahren, im Vergleich zu symmetrischen Verfahren, sehr rechenaufwändig. Um kurze Nachrichten zu verschlüsseln, benötigt der Computer viel Zeit. Deshalb bedient man sich eines Tricks: Mit dem langsamen, asymmetrischen Verfahren werden nur die Schlüssel für ein schnelles symmetrisches Verfahren sicher und unkompliziert ausgetauscht. Die weitere Kommunikation erfolgt dann über die schnellere symmetrische Verschlüsselung. Weil asymmetrische Verfahren dafür genutzt werden, die Schlüssel eines symmetrischen Verfahrens zu verschlüsseln, nennt man es hybride - also kombinierte - Verschlüsselung.

- Zweitens kann keiner so leicht rauskriegen, ob der verwendete Public Key auch wirklich demjenigen gehört, dem man die verschlüsselte Nachricht schicken will. Im Internet ist es leicht sich für jemanden anderen auszugeben und es könnte jemand fälschlicherweise behaupten, er wäre der berechtigte Empfänger und Ihnen seinen Public Key andrehen wollen. Er könnte dann die vertrauliche Botschaft lesen. Würde er sie danach, vielleicht auch noch gefälscht, an den richtigen Empfänger weiterleiten, bliebe das ganze wahrscheinlich auch noch unbemerkt.

Diese Problematik lässt sich mithilfe einer **Public Key Infrastructure** (PKI) verhindern.

3. PKI und Digitale Signatur:

Besonderes Merkmal der **Public Key Infrastructure** (PKI) ist die **Zertifizierungstelle**. Das ist eine allgemein anerkannte Stelle, deren Aufgabe es ist, die jeweils **einmaligen Schlüsselpaare** (privater und öffentlicher Schlüssel) natürlichen Personen fest zuzuordnen und dies den Benutzern mittels **"Zertifikaten"** zu bestätigen.

Vereinfacht funktioniert das ganze so: Jeder Benutzer kennt den Public Key der Zertifizierungsstelle. Aber nur sie hat den passenden Private Key für eine sinnvolle Verschlüsselung als Gegenstück dazu. Jetzt erfolgt das Gegenteil vom bisherigen

Verschlüsseln einer Nachricht. Die Zertifizierungsstelle erstellt einen Text, in dem der öffentliche Schlüssel einer Person zugeordnet wird, und verschlüsselt dies aber mit ihrem geheimen Schlüssel. Weil der öffentliche Schlüssel der Zertifizierungsstelle allen bekannt ist, kann diesen Text auch jeder lesen.

Und wozu das ganze? Jeder weiß nun genau, dass die Zertifizierungsstelle diesen Text geschrieben hat - nur sie kann mit ihrem Private Key Nachrichten so verschlüsseln, dass mit dem allen bekannten Public Key wieder eine sinnvolle Nachricht dabei herauskommt. In diesem Fall hat die Zertifizierungsstelle eine Nachricht geschrieben und digital mit ihrem privaten Schlüssel "signiert". Sofern Sie der Zertifizierungsstelle vertrauen, können Sie dann auch darauf vertrauen, dass dieser Public Key einer ganz bestimmten Person gehört.

Die so erfolgte digitale Signatur ist also keine digitalisierte "echte" Unterschrift, sondern ein Bitmuster, das mittels eines mathematischen Verfahrens erstellt wird. Eine digitale Signatur können auch Sie erstellen, wenn Sie ein gültiges Schlüsselpaar aus öffentlichen und privaten Schlüssel besitzen. Sie brauchen aber die Zertifizierungsstelle, die bestätigt, dass Sie und kein anderer zu Ihrem Public Key gehören.

Mithilfe der PKI können Sie nicht nur Nachrichten sicher verschlüsseln, um deren Inhalt vor neugierigen Zeitgenossen zu verbergen. Die digitale Signatur verhindert auch, dass Nachrichten unbemerkt verändert werden.

Sehen Sie sich einfach diesen Text mit der anschließenden Zahl an:

[Angriff im Morgengrauen 21/207]

Die 21 steht für die Anzahl der Buchstaben im Text und die 207 für den Wert der Buchstaben, wenn man diese nach Ihrer Stellung im Alphabet addiert. Aus dem Text lassen sich die Zahlen leicht ermitteln, aber nicht umgekehrt. Mithilfe der PKI kann man den Text und die Zahlen verschlüsseln und mit der Nachricht gleich mitschicken. So wird der Empfänger merken, ob irgend etwas manipuliert wurde. Sonst würden die Zahlen nicht mehr zum Text passen. Allerdings gibt es dabei noch einen Haken: Wer den Text manipuliert, kann natürlich auch die so Zahlen manipulieren, dass sie wieder zum Text passen. Damit das nicht passiert, werden die Zahlen mit dem geheimen Schlüssel des Absenders verschlüsselt. Das noch genauer zu erklären, würde an dieser Stelle aber nun wirklich zu weit führen.

Kombiniert man schließlich alles, erhält man ein tolles Ergebnis: Niemand kann unbemerkt die Nachrichten fälschen, lesen oder sich für jemanden anderen ausgeben. Das ist doch prima, oder?

Anwendung der Verschlüsselungsverfahren

Viele private Nutzer verwenden das Programm **Pretty Good Privacy -** abgekürzt **PGP** (deutsch: ganz gute Vertraulichkeit) - für die Verschlüsselung ihrer E-Mails und Dateianhänge. PGP beruht einem **hybriden Verschlüsselungsverfahren**: Um Nachrichten zu verschicken, werden diese mit dem entsprechenden öffentlichen Schlüssel des Adressaten verschlüsselt. Der kann die Nachricht dann mit dem geheimen Schlüssel dechiffrieren.

Neben dieser kommerziellen Software gibt es auch noch **GnuPG** (**GNU P**rivacy **G**uard). Das ist das erste mit Bundesmitteln geförderte Freie Software Projekt. Mit dieser Open-Source-Software kann man ebenfalls E-Mails und Dateien sicher, vertrauenswürdig, einfach und kostenlos verschlüsseln - unabhängig von den jeweiligen Datenformaten (E-Mail, Textdateien, Bilddaten, usw.). GnuPG ist kompatibel zu PGP, das heißt mit GnuPG verschlüsselte E-Mails können mit PGP entschlüsselt werden und umgekehrt. GnuPG verwendet dazu hauptsächlich ein hybrides Verfahren und arbeitet mit Public Keys. Zum Verschlüsseln kann GnuPG aber wahlweise ausschließlich mit symmetrischen Verfahren eingesetzt werden.

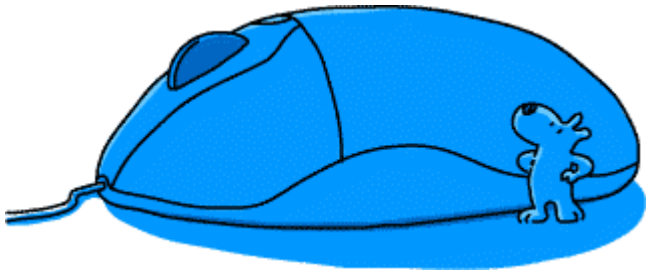
Eventuell haben Sie in diesem Zusammenhang auch schon einmal etwas von GnuPP (GNU Privacy Projects) gehört. GnuPP ist ein Projekt, dass die Verwendung von GnuPG auf dem am meisten verbreiteten Betriebssystem Windows vereinfachen will. Denn GnuPG ist eine so starke Verschlüsselungstechnologie, dass eine breite Öffentlichkeit - also auch alle Windows-Anwender - sie in Zukunft nutzen soll.

Zum Schluss noch zu "echten" Anwendungen der **Digitalen Signatur** (oder juristisch korrekt der "Elektronischen Signatur"): Wie bereits gesagt, soll durch sie der Ersteller eines elektronischen Dokuments erkennbar sein und die Dokumente vor unbemerkten Veränderungen geschützt werden. Die mit der elektronischen Signatur unterschriebenen Rechtsgeschäfte (Verträge, Steuererklärungen, etc.) sollen natürlich auch dauerhaft und beweisbar rechtsgültig sein. Deshalb wurden im Signaturgesetz Qualitätsstufen festgelegt. Die regeln die dafür notwendigen Details. **Die im Signaturgesetz definierte qualifizierte elektronische Signatur ist durch Gesetzesänderungen zukünftig auch formal als Ersatz der eigenhändigen Unterschrift zugelassen**. In zahlreichen Pilotversuchen in Wirtschaft und Verwaltung wird diese neue Technologie derzeit schon erprobt.

Das waren jetzt ziemliche viele Informationen auf einmal. Vielleicht konnten wir Sie aber davon überzeugen, dass das mit der Verschlüsselung eine ganz nützliche Sache ist. Wenn Sie wollen, können Sie es auch gleich selbst ausprobieren: In der Toolbox finden Sie ein Verschlüsselungsprogramm. Dann sehen Sie gleich, wie es in der Praxis funktioniert. **Zur Erinnerung**: Die Sicherheit Ihrer Nachrichten hängt von der Wahl eines originellen - also schwer zu erratenden - und nicht zu kurzen Schlüssels ab.

Quelle: http://www.bsi-fuer-buerger.de/08/

Kinderschutz



Kinder gehören zu den **aktivsten Nutzern der neuen Technologien**. Der Umgang mit dem Medium Internet ist für viele von ihnen bereits selbstverständlich. Mit einem PC und Internetzugang können Kinder mit Freunden chatten, neue Leute kennen lernen, Spiele - auch gegen wirkliche Gegner - spielen. Sie können Filmausschnitte gucken, Musik hören, Videospiele ausprobieren oder herunterladen, Fremdsprachen erlernen und neue Interessen entwickeln. Kurz gesagt: **Das Internet bietet Kindern ungeahnte Möglichkeiten und es gibt keinen Zweifel daran, dass die meisten davon sinnvoll sind**. Bevor Sie Ihr Kind jedoch auf die Datenautobahn schicken, sollten Sie ihm sozusagen einen "Sicherheitsgurt" anlegen.

Welche Gefahren gibt es?

Zahlreiche Internetseiten sind für jüngere Menschen nicht geeignet. Besonders Seiten über Sex, Rassismus und Gewalt stellen eine Bedrohung dar. Weil das Internet jedoch global und dezentralisiert ist, können die Inhalte nur schwer kontrolliert werden. Zusätzlich versucht täglich eine große Anzahl Pädophiler über das Internet Kontakt zu Kindern und Jugendlichen aufzubauen. So genannte Selbstmordforen, die Möglichkeit über das Internet an Drogen zu gelangen oder durch Unachtsamkeit beim Internetsurfen einen 0190-Dialer auf dem PC zu installieren, sind nur drei von vielen weiteren Gefahren, die Ihrem Kind im Internet begegnen können.

Darüber hinaus ist das Internet ein persönlich ansprechendes Medium, das Experten zufolge Kinder in einen "Schwebezustand" versetzen kann, der sie für Werbung sehr empfänglich macht. Es sind subtilere Marketingmethoden möglich, die Kinder zum Kaufen animieren können. Von den 100 am häufigsten aufgerufenen Seiten für Kinder und Jugendliche sind nur rund zehn Prozent nicht kommerzieller Natur.

Um Ihr Kind vor diesen Gefahren zu schützen, können Sie den **Internetzugang Ihres Kindes entweder unterbinden, filtern** beziehungsweise zensieren, **oder Sie protokollieren alles**, was sich Ihr Kind im Internet ansieht. Dazu gibt es zahlreiche **Software, die versucht, die "guten" von den "schlechten Seiten" zu trennen**.

Was macht eine Filter-Software?

Die Filter-Software sperrt anhand von Schlüsselwörtern bestimmte Internetseiten. Die Seiteninhalte werden dann nicht mehr dargestellt. Zudem erstellen die Softwarehersteller so genannte **Negativlisten**. Darauf sind einschlägig bekannte Internetadressen zu jugendgefährdenden Inhalten vermerkt. Es gibt auch **Positivlisten** mit Seiten, die immer besucht werden dürfen. Die Software kann aber noch mehr: Sie protokolliert zusätzlich, welche Seiten tatsächlich aufgerufen werden. So können Sie die Negativliste im Nachhinein an den persönlichen Bedarf Ihres Kindes anpassen. Bei den meisten Programmen lässt sich außerdem die Zeitdauer festlegen, die ein Benutzer im Internet surfen darf. Viele Schutzprogramme kommen allerdings aus den USA. Sie suchen in erster Linie nach englischen Schlüsselwörtern und blockieren kaum deutsche Seiten. Dem können Sie entgegenwirken, indem Sie ein deutschsprachiges Programm verwenden.

Wenn Sie die Filter-Software auf Ihrem lokalen Rechner installieren, nehmen Sie auch dort die Konfiguration vor. So bleiben Ihre Daten vertraulich und Sie können das Programm optimal an Ihre individuellen Bedürfnisse anpassen. Allerdings erfordert diese genaue Einstellung Zeit und muss permanent gepflegt werden. Es gibt aber noch eine andere Möglichkeit: Sie können auch ein Programm verwenden, das bereits in das Angebot eines Internetserviceproviders eingebunden ist. (z.B. AOL, Compuserve, etc.). Die Filterkriterien und - listen sind dann zwar nicht mehr individuell auf Sie zugeschnitten, aber Sie ersparen sich so die Pflege der Einstellungen, die von einer zentralen Stelle des Internetproviders übernommen wird.

Einige Filterprogramme basieren auf der vom World Wide Web Consortium entwickelten Platform for Internet Content Selection (PICS). Dabei klassifizieren die Anbieter ihre Inhalte selbst, zum Beispiel als Werbung. Anschließend werden die Seiten mit einem Etikett versehen, das Hinweise zu den Inhalten enthält. Das Problem ist allerdings, dass sich die Inhalte von WWW-Seiten nicht so einfach klassifizieren lassen wie beispielsweise die Zutaten von Lebensmitteln.

Allerdings gibt es im Internet ja nicht nur Webseiten, sondern auch jede Menge anderer Informationsquellen. Effektive Filtersoftware sollte daher nicht nur den Browser überwachen, sondern auch die anderen Programme, wie z. B. Chat- und E-Mail-Programme (z.B. Outlook Express) berücksichtigen. Besonders in Chats oder den Diskussionsforen wie Newsgroups wimmelt es von jugendgefährdenden Inhalten.

Wenn Sie sich dafür entscheiden, ein solches Filter-Programm auf Ihrem Rechner zu installieren, dann sollten Sie **folgende Punkte beachten:**

- Der Funktionsumfang des Programms ist anhand der Positiv- und Negativlisten sowie der Qualität der Schlüsselwörter erkennbar.
- Die Listen sollten an Ihre Bedürfnisse anpassbar sein.
- Die Software sollte in der Lage sein, sich an den konkreten Bedarf anzupassen: Die Altersgruppe, die verschiedenen Sicherheitsanforderungen und Wertvorstellungen müssen berücksichtigt werden können. Es sollte auch möglich sein, mehrere Benutzer mit unterschiedlichen Anforderungen zu bestimmen.
- Gute Software lässt sich durch Downloads aktualisieren.

Wenn das Programm diese Kriterien erfüllt, dann ist zumindest die technische

Unterstützung des Jugendschutzes weitgehend umgesetzt.

Sollten Sie kein eigenes Programm installieren wollen, bietet Ihnen der Internet-Explorer die Möglichkeit unter den Menüpunkten "Extras", "Internet-Optionen", "Inhalte" den so genannten Inhalteratgeber zu aktivieren. Damit können Internetseiten ausgeblendet werden, die sich selbst als Seiten mit Gewalt, Sex oder freizügiger Sprache eingeordnet haben. Der Haken dabei ist, dass nicht eingeordnete Seiten entweder vollständig angezeigt oder blockiert werden.

Für alle Maßnahmen gilt jedoch eines: **Viele Kinder kennen sich mit dem PC besser aus als ihre Eltern**. Die meisten Programme lassen sich einfach deinstallieren und im Internet gibt es darüber hinaus einschlägige Seiten, auf den beschrieben ist, wie die Filterprogramme umgangen werden können. Und egal, welche Schutzmaßnahmen Sie treffen, alle sind mit dem Problem der Unüberschaubarkeit und Schnelligkeit des Internets konfrontiert. **Deshalb können technische Schutzmaßnahmen lediglich ein Baustein in einer Reihe weiterer Maßnahmen sein**. Dazu gehört eine umfassende Medienerziehung sowie feste Regeln, die Sie Ihrem Kind mit auf den Weg geben können, wenn es im Internet surft. Ihr Kind sollte den verantwortungsvollen Umgang mit dem PC und dem Internet lernen und zum Beispiel wissen, dass es die Wohnanschrift, die Telefonnummer oder andere private Daten nicht an Unbekannte weitergibt. Natürlich sollten Sie Ihrem Kind auch Vorbild sein und den verantwortungsbewussten Umgang mit dem Internet vorleben.

Rechtliche Folgen

Vielen Kindern und Jugendlichen fehlt im Umgang mit dem Internet das Bewusstsein für mögliche - teils auch immense zivilrechtliche - Folgen. Wenn es um Delikte im Bereich Hacking sowie um das Erstellen von Raubkopien geht, sind sie überrepräsentiert. Grund dafür ist **fehlendes Unrechtsbewusstsein**. Und so mancher Jugendlicher löst einen DoS-Angriff aus, ohne sich über die Folgen im Klaren zu sein. Auch hier sollten Sie mit Ihrem Kind über mögliche Folgen sprechen.

Quelle: http://www.bsi-fuer-buerger.de/09/

Der Staat online

Wer kennt diese Situation nicht: Sie stehen in einem Amt, haben einen Bogen mit vielen Fragen vor sich und stellen fest, dass Ihnen zum ordnungsgemäßen Ausfüllen Unterlagen fehlen. Ihnen bleibt also nichts anderes übrig, als noch einmal zum Amt zu gehen. Ärgerlich. Wie schön wäre es doch, den Bogen in aller Ruhe zu Hause am Bildschirm auszufüllen und ihn als elektronische Post zum zuständigen Amt zu schicken. Zukunftsmusik denken Sie? Nicht ganz. **E-Government** heißt das Zauberwort und steht für **Electronic Government**, die elektronische Verwaltung. Dabei werden die Daten des Bürgers oder eines Unternehmens direkt vom eigenen PC über das Internet in die IT-Systeme der Behörde übertragen und dort verarbeitet.

"Die Daten sollen laufen, nicht die Bürger." sagte Bundeskanzler Gerhard Schröder und startete im Oktober 2000 die Initiative BundOnline 2005 www.bundonline2005.de/. Danach verpflichtet sich die Bundesregierung **bis 2005 alle online-fähigen Dienstleistungen der Bundesverwaltung für Bürger, Unternehmen und Verwaltungen im Internet anzubieten**. Dafür investiert der Bund 1,65 Milliarden Euro. Durch den Einsatz moderner Informations- und Kommunikationstechnik wird so die Entstehung einer "digitalen" Verwaltung möglich. Manche Gänge zur Behörde werden deshalb in Zukunft überflüssig.

Was können Sie bereits online erledigen?

Die erste Stufe von E-Government besteht aus allgemeinen - aber in der Regel sehr nützlichen - Informationsangeboten, die ohne Sicherheitsprobleme bereitgestellt und abgerufen werden können. Fast alle Bundesbehörden, Länder und Kommunen haben inzwischen solche Angebote und bieten sie auf ihren Internetseiten für den Bürger an. Dazu gehört die Bekanntgabe der Schwimmbadöffnungszeiten genauso wie beispielsweise das Herunterladen von bestimmten Formularen im virtuellen Rathaus.

Etwas komplizierter wird es, wenn "echte" Online-Dienstleistungen durchgeführt werden sollen, Sie also zum Beispiel einen Antrag online stellen wollen. Aber auch hier gibt es durchaus einige interessante Beispiele: In Bremen (www.bremer-online-service.de) können Sie mit Hilfe der elektronischen Signatur sicher und rechtsverbindlich den Stadtwerken Ihren Zählerstand mitteilen oder beim Standesamt eine Heiratsurkunde bestellen. Die Stadt Esslingen bietet Signaturinhabern die Online-Anmeldung zur Hundesteuer und die Online-Baugenehmigung. Und in Nürnberg kann man seinen Anwohnerparkausweis im Internet bestellen.

Der Bund selbst geht auch mit gutem Beispiel voran: Auf der CeBIT 2001 wurde das Dienstleistungsportal des Bundes frei geschaltet. Noch erhalten die Bürger unter www.bund.de in erster Linie nur Informationen, so zum Beispiel einen Überblick über alle Behörden, Informationen zu allen Bundesländern und Kommunen, ein Formular-Center usw. Es gibt aber auch schon "echte" Online-Dienstleistungen: Dazu gehört bespielsweise das Projekt "Elektronische Steuererklärung" (www.elster.de). Dabei wurden schon rund 300.000 Steuererklärungen elektronisch versendet. Und auch der Internet-Banking-Service der Bundeswertpapierverwaltung (https://www.bwpv-direkt.de), der rund 1,3 Millionen Konten verwaltet, ist eine von zukünftig sehr vielen elektronischen Dienstleistungen des Bundes.

Wie Sie Ihre Daten an die Behörde übermitteln

Als Bürger, Unternehmen oder anderer Kunde der Verwaltung erwarten Sie natürlich, dass Ihre persönlichen Daten bei der Übertragung durch das Internet genauso sicher sind und von der Verwaltung ebenso sorgfältig behandelt werden wie sonst auch.

Der Faktor IT-Sicherheit entscheidet deshalb ganz wesentlich darüber, ob die E-Government-Angebote genutzt und akzeptiert werden.

Damit Sie mit der Verwaltung über das Internet kommunizieren können, müssen die bisher abgeschotteten behördeninternen IT-Systeme nach außen "geöffnet" werden. Ihr PC hat damit eine - mehr oder weniger - direkte Verbindung zu den Hintergrundsystemen der meisten Behörden. Das heißt aber natürlich noch lange nicht, dass Sie ohne Weiteres auf die dort gespeicherten Daten zugreifen können. Die Behörden stellen jederzeit sicher, dass unberechtigte Anfragen durch unterschiedliche technischen Maßnahmen, wie zum Beispiel den Einsatz von Firewalls, zuverlässig unterbunden werden.

Dabei kommt es besonders auf **zwei Aspekte** an:

• Bevor ein Kunde personalisierte Angebote in Anspruch nehmen kann, muss geprüft werden: Inwiefern ist er berechtigt, gewisse Aktionen zu veranlassen oder auf gewisse Daten zuzugreifen? In der Fachsprache heißt das Authentisierung. Dazu können bestimmte Mechanismen - wie zum Beispiel das PIN-TAN-Verfahren - eingesetzt werden. Oder auch die, allerdings noch nicht sehr verbreiteten, elektronischen Signaturen.

• Werden persönliche Daten über das Internet übertragen, so muss auch die Vertraulichkeit der Daten sichergestellt werden (Datenschutz). Niemand möchte wohl, dass sein Nachbar oder Chef alle mit Behörden ausgetauschten Daten mitlesen kann. Vertraulichkeit zu wahren ist technisch eine einfache Aufgabe: Alle Daten müssen

verschlüsselt werden. Innerhalb des Webs kann dies, fast automatisch, durch die Nutzung von sicheren Internetseiten - so genannten SSL-Seiten - geschehen. Bei E-Mails hingegen ist etwas mehr Aufwand zu betreiben, dafür benötigen Sie Verschlüsselungssoftware.

Haben Sie sich jedoch erst einmal an den Umgang mit Verschlüsselungssoftware und Authentisierungsmechanismen (Signaturen, etc.) gewöhnt, werden Sie schnell sehen, dass **E-Government** gar nicht kompliziert ist und **Ihnen viel Zeit spart.**

Quelle: http://www.bsi-fuer-buerger.de/10/

Online-Banking

Führen Sie Ihr Konto auch schon online über das Internet? Wenn ja, dann gehört Ihnen eins der **20 Millionen Konten**, die Ende 2001 in Deutschland online geführt wurden. Dabei hat sich die Zahl der Online-Konten in den letzten fünf Jahren verfünffacht. Ist ja auch logisch - immer mehr Menschen haben das Internet für sich entdeckt und finden es praktisch ihre **Bankgeschäfte von zu Hause oder von unterwegs** erledigen zu können. Neben den Vorteilen und Möglichkeiten, die Ihnen das Internet dabei bietet, gibt es aber auch **verschiedene Risiken**. Die können Sie jedoch selbst minimieren, wenn Sie einige **Sicherheitsvorkehrungen** beachten.

Online-Banking - was heißt das?

Gemeint sind alle Bankgeschäfte, die Sie mit Ihrem PC über das Internet abwickeln.

Neben dem Internetbanking gibt es auch Telefon- und Homebanking. Dabei haben alle diese Bankgeschäfte gemeinsam, dass Geschäftsvorfälle von der Bankfiliale zu den Kunden verlagert werden.

Telefonbanking

Beim Telefonbanking ruft der Kunde die Servicenummer seines Kreditinstituts an. Die Bank nimmt die Aufträge entgegen und bearbeitet sie. Dabei gibt es verschiedene technische Varianten: Entweder sprechen Sie mit einem Menschen, nur mit einem Computer und steuern alles über die Telefontastatur oder aber beides ist miteinander kombiniert. Da man am Telefon den jeweiligen Auftrag nicht unterschreiben kann, werden die Transaktionen über Passwörter abgesichert. Da Telefongespräche abgehört werden können, birgt das Telefonbanking ein großes Sicherheitsrisiko.

Homebanking

Der Begriff Homebanking wird oftmals synonym zum Internetbanking gebraucht. Er meint technisch gesehen aber etwas anderes. Um Ihre Bankgeschäfte erledigen zu können, ist Ihr PC beim Homebanking über Btx an den Rechner Ihres Kreditinstituts angebunden. Sie können Homebanking aber auch über das Internet durchführen. Dazu ist der Homebanking Computer Interface Standard (HBCI) entwickelt worden. Vorteil von Btx ist das geschlossene System. Dadurch ist es weitgehend sicher.

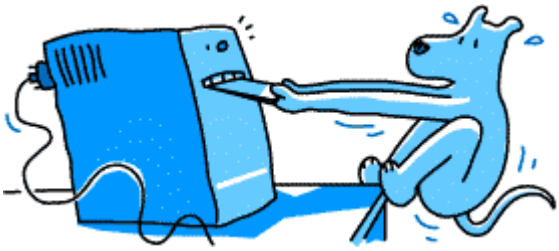
Internetbanking

Auf den ersten Blick unterscheidet sich Homebanking vom Internetbanking durch die grafische Öberfläche. Btx ist mit seiner zeichenorientierten Oberfläche nämlich schon ein wenig in die Jahre gekommen. Beim Internetbanking bietet Ihnen Ihre Banke den Kontenzugriff über das Internet an. Die Verfahren, die dabei im Hintergrund ablaufen, sind dabei aber weitgehend dieselben wie beim Homebanking über Btx. In den meisten Fällen wird für Internet-Banking das PIN-TAN-Verfahren eingesetzt, bisher nur vereinzelt HBCI. Tendenziell sind in letzter Zeit immer mehr Benutzer vom Homebanking auf das Internetbanking umgestiegen.

Wie schützen Sie sich vor den Sicherheitsrisiken beim Internetbanking?

Alle Gefahren, die Ihnen auch sonst im Internet drohen gibt es natürlich auch bei Bankgeschäften über das Internet. Ihre Daten können bei der Übertragung ausspioniert, verändert oder sogar gelöscht werden.

Dabei treffen die Banken eine Reihe von Sicherheitsvorkehrungen, die in der Regel einen wirksamen Schutz bieten. Die Daten werden zum Beispiel meistens verschlüsselt. Häufig wird dafür das in den meisten Browsern ohnehin integrierte SSL-Protokoll eingesetzt.



Aber auch Sie als Kunde müssen Sicherheitsvorkehrungen treffen. Wenn Sie folgende zehn Regeln beachten, können Sie Ihr Risiko auf eine Minimum reduzieren:

10 Tipps

1. Bestehen Sie auf eine Verschlüsselung Ihrer Daten, zum Beispiel über SSL

2. Vergewissern Sie sich, mit wem Sie es beim Internetbanking zu tun haben. Achten Sie genau auf die URL und das SSL-Zertifikat!

3. Schützen Sie Ihre Kennwörter und Zugangsdaten! Speichern Sie diese auf keinen Fall auf Ihrem Rechner und verwahren Sie sie so, dass niemand darauf zugreifen kann.

4. Wählen Sie kein Allerweltspasswort, sondern verwenden Sie möglichst schwer zu ratende Passwörter. Beim Online-Banking können meist nur numerische Passwörter gewählt werden, so dass gute Passwörter nur schwer zu merken sind. Nehmen Sie aber trotzdem auf keinen Fall Ihr Geburtsdatum! Wechseln Sie Ihr Passwort regelmäßig.

5. Aktivieren Sie die Sicherheitseinstellungen des Browsers! Achten Sie darauf, dass Ihr

Internet-Browser alle aktuellen Sicherheitsfunktionen beinhaltet.

6. Verwenden Sie Sicherheitssoftware, zum Beispiel Virenscanner.

7. Fertigen Sie regelmäßig Sicherheitskopien Ihrer Daten an.

8. Überprüfen Sie Ihre Kontobewegungen regelmäßig!

9. Vereinbaren Sie mit Ihrer Bank ein Limit für die täglichen Geldbewegungen über Online Banking. Falls Unbefugte auf Ihr Konto zugreifen, können Sie den Schaden damit zumindest begrenzen.

10. Kommt Ihnen beim Internetbanking irgendetwas komisch vor, sperren Sie Ihren Internetbanking-Zugang über das Sperrpasswort und setzen Sie sich so schnell wie möglich mit Ihrem Kreditinstitut in Verbindung.

Quelle: http://www.bsi-fuer-buerger.de/11/

Open-Source-Software

Dieser kleine Pinguin ist Ihnen sicher schon einmal irgendwo über den Weg gelaufen. Vielleicht wissen Sie ja auch schon, dass er **Tux** heißt und das Maskottchen des **Betriebssystems Linux** ist. Was sich jedoch hinter Linux und dem Begriff **Open-Source-Software** verbirgt, war Ihnen bislang ein Rätsel. Nun ja, auch Rätsel können gelöst werden ...
Fangen wir doch mit den folgenden sieben Antworten einfach damit an:

Fragen & Antworten zu Open-Source-Software

Was heißt Open-Source-Software (OSS)?
Wann ist eine Software eine Open-Source-Software?
Warum gibt es Open-Source-Software?
Ist Open-Source-Software genauso sicher wie proprietäre Angebote?
Wer ist bei Problemen mit Open-Source-Software zuständig?
Beispiele für Open-Source-Software
Und zum Schluss: Ist Open-Source-Software immer kostenlos?

Was heißt Open-Source-Software (OSS)?

Damit Ihr PC ein Programm ausführen kann, muss er die Programmiersprache der Entwickler in eine Maschinensprache übersetzen. Bei einem proprietären, das heißt herstellergebundenen, Programm wird nur diese ausführbare Form ausgeliefert. Dadurch ist das Programm an eine ganz bestimmte Architektur des Computers gebunden - zum Beispiel an einen handelsüblichen PC mit einem Prozessor einer ganz bestimmten Marke. Sie als Anwender können das Programm weder prüfen noch verändern. Sie dürfen und können es noch nicht einmal lesen. Die von den Entwicklern geschriebene "ursprüngliche" Form heißt "Quellcode" oder englisch "Source Code". Er beschreibt alle Leistungen des Programms vollständig.

Open-Source-Software unterscheidet sich von proprietärer Software grundlegend darin, dass auch der Quellcode erhältlich ist. Sie als Anwender können das Programm also unabhängig von seinen Autoren in der Regel beliebig verändern. Sie können es auch weitergeben und erkannte Schwachstellen oder Fehler veröffentlichen. Weil der Quellcode jedem offen zugänglich ist, wird solche Software Open-Source-Software oder auch Freie Software genannt.

Wann ist eine Software eine Open-Source-Software?

Erfüllt eine Software folgende Kriterien, darf sie sich "Open-Source-Software" nennen.

Bei Open-Source-Software dürfen Sie im Normalfall:

- untersuchen, wie ein Programm funktioniert, weil Ihnen der Quellcode offen steht
- das Programm den eigenen Bedürfnissen anpassen, verbessern und diese

Verbesserungen zum allgemeinen Wohl zugänglich machen.
- auf entdeckte Fehler und Schwachstellen öffentlich hinweisen.
- Kopien für Andere machen, wobei Sie keine Lizenzgebühren verlangen dürfen.

Warum gibt es Open-Source-Software?

Die Philosophie von Open-Source-Software geht zurück auf den Grundgedanken des freien Austauschs von Wissen und Gedanken. Software kann, wie auch Ideen, jedem frei zur Verfügung gestellt werden - ohne Verluste. Wird Software weitergeben, entwickelt sie sich wie in einem evolutionären Prozess.

Ein Beispiel:

Nehmen wir an, Sie brauchen eine Software, die es aber nicht zu kaufen gibt. Sie müssen also selbst eine Software entwickeln, testen und haben allen Aufwand, den so etwas mit sich bringt. Eigentlich würde es Ihnen aber nichts ausmachen, wenn auch andere das Programm benutzen würden. Im Gegenteil, Sie würden sogar von der Erfahrung und von der Beteiligung weiterer Nutzer profitieren. Grund genug, Ihr Software-Projekt zu beginnen und es sobald wie möglich als Open-Source-Projekt zu unterstützen. Sie geben dann Ihr Programm für die Verwendung frei und profitieren im Austausch von der zusätzlichen Kapazität und Expertise der anderen Entwickler und Anwender. Dabei kann es Ihnen egal sein, ob nur ein kleiner Teil oder alle Anwender zur weiteren Entwicklung beitragen.

Daneben gibt es noch eine andere Überlegung: Warum sollen Projekte, die beispielsweise aus Steuermitteln finanziert werden, also von allen bezahlt werden, nicht auch wieder allen zugute kommen?

Ist Open-Source-Software genauso sicher wie proprietäre Angebote?

Ja. Weil viele Programmierer in aller Welt - man nennt sie "Community" oder Entwickler-Gemeinschaft - die Möglichkeit haben, sich den Quelltext der Software anzusehen, können mögliche Probleme rasch erkannt und gegebenfalls sofort behoben werden. Denn: Viele Augen sehen viel! Die Entwickler sind normalerweise namentlich bekannt. Keiner von ihnen würde sich gerne nachsagen lassen, er habe schädliche Software programmiert.

Ein weiterer Sicherheitsaspekt ist, dass Open-Source-Software bislang selten von Viren befallen wird. Das liegt natürlich zum einen daran, dass sie noch nicht so stark verbreitet ist wie proprietäre Software. Zudem waren die Sicherheitsfunktionen bei Freier Software bis jetzt auch größer. Die Programme sind ausserdem von überflüssigem Schnick-Schnack frei.

Wer ist bei Problemen mit Open-Source-Software zuständig?

Ist ja alles schön und gut, könnten Sie denken, aber was, wenn ich einmal Probleme mit Freier Software habe. Fühlt sich denn da überhaupt jemand verantwortlich, wenn eigentlich alle mit entwickeln? Keine Sorge, es gibt sogar Untersuchungen die beweisen, dass die Unterstützung für Open-Source-Software oft besser ist als die für herstellergebundene proprietäre Angebote. Experten können auch komplexe Probleme mit Hilfe der Community schnell lösen. Bei proprietärer Software ist es nötig, erst das Entwicklungsteam des Herstellers zu kontaktieren - und das kann bekanntlich auch mal

länger dauern.

Beispiele für Open-Source-Software

Inzwischen ist Open-Source-Software eine anerkannte Alternative zu proprietären Angeboten. Besonders die Europäische Union und zahlreiche öffentliche Verwaltungen unternehmen erhebliche Anstrengungen, um den Einsatz von Open Source Systemen zu fördern. Auch große Konzerne wie etwa IBM, Hewlett Packard oder Sun sind Förderer von Open Source Systemen und Entwicklungen. Selbst prominente Hersteller proprietärer Software wie Oracle oder SAP haben zahlreiche Berührungspunkte zur Open-Source-Bewegung oder bieten ihre Produkte zumindest auch für das Betriebssystem Linux an.

Deshalb gibt es mittlerweile auch viele Programme, die als Open-Source-Software angeboten werden. Neben Tools für die Programmentwicklung und für die professionelle Betreuung von Servern und Netzwerken gibt es eine Fülle von Anwendungsprogrammen für den täglichen Einsatz im Unternehmen oder anderswo.

Einige Beispiele:

- Linux ist ein sehr leistungsfähiges Betriebssystem für eine Vielzahl von Plattformen und ist das Paradebeispiel für ein erfolgreiches Open-Source-Projekt. Erfunden hat es 1991 der damals 21-jährige Linus Torvalds. Seither wird es von einer Vielzahl an Entwicklern aus aller Welt weiterentwickelt. Prominentes Beispiel für den Stellenwert von Linux ist der Deutsche Bundestag. Im Serverbereich wird dort zukünftig Linux und andere Open-Source-Software eingesetzt.

- Der Internetbrowser Mozilla ist ebenfalls für verschiedene Betriebssysteme verfügbar. Der Quellcode stammt ursprünglich von Netscape.

- Der Web-Server Apache zählt neben Linux zu den erfolgreichsten Open-Source-Projekten. Mehr als die Hälfte aller Web-Server arbeiten mit dieser Software.

Und zum Schluss: Ist Open-Source-Software immer kostenlos?

Nein, genau das ist auch das häufigste Missverständnis in bezug auf Open-Source-Software. Man kann die Software kostenlos aus dem Internet beziehen, bezahlt aber die Kosten für das Herunterladen selbst. Je nachdem, welche Art von Internetanschluss Sie verwenden, kann es unter Umständen billiger sein, das Programm auf CD zu kaufen. Sie bezahlen dann für das Bereitstellen der Software auf CD, aber nicht für den Gebrauch der Software selbst.

Zudem muss ein freies Programm für den kommerziellen Gebrauch, die kommerzielle Entwicklung und für die kommerzielle Verteilung zur Verfügung stehen. Die kommerzielle Entwicklung von Open-Source-Software ist nicht mehr unüblich; oft wird Open-Source-Software für kommerzielle Zwecke entwickelt. Somit sind auch nicht alle

Formen von kostenlos nutzbarer Software Open-Source-Software.

Einige Beispiele anderer kostenloser Vertriebsformen sind:

- Freeware ist Software, die kostenlos genutzt werden kann. Andere Nutzungskriterien wurden bislang nicht definiert. Aber Vorsicht: Damit schleichen sich gern Viren, Trojanische Pferde oder andere Schädlinge ein!

- Shareware kann zunächst frei installiert werden. Später kann der Autor für die Nutzung oder für bestimmte Formen der Nutzung Lizenzkosten verlangen. Der Autor verzichtet lediglich auf die Prüfung oder auf Maßnahmen zur Sicherstellung dieser Lizenzzahlungen. Manchmal steht Anwendern bis zur Bezahlung der Lizenzen - also bis zur Registrierung - nur ein reduzierter Funktionsumfang zur Verfügung.

- Probesoftware kann nur für eine bestimmte Zeit kostenlos genutzt werden und unterliegt dann üblichen kommerziellen Lizenzformen oder ist Shareware.

Quelle: http://www.bsi-fuer-buerger.de/12/

Recht im Internet

Auch im Internet gibt es Spielregeln. Zahlreiche Gesetze regeln Recht und Unrecht. Zwei besonders oft diskutierte Themen sind der **Datenschutz** und die **Internetkriminalität**.

Jetzt fragen Sie sich im ersten Moment vielleicht, was Sie das angeht, schließlich wollen Sie nur im Internet surfen und E-Mails schreiben. Allerdings kommen Sie am Datenschutz nicht vorbei, es sei denn Ihnen ist Ihre Privatsphäre völlig gleichgültig. Aber in Ihr Wohnzimmer lassen Sie ja auch nicht jeden herein, oder? Deshalb sollten Sie wissen, wie Sie verhindern können, dass Ihre Daten ohne Ihr Einverständnis weitergegeben werden.

Ein anderes wenig erfreuliches Thema ist die **Kriminalität im Internet**. Zum Glück wimmelt es im Internet nicht nur von Kriminellen, doch **schwarze Schafe gibt es überall**. Welche Straftaten es genau gibt, wie Sie sich gegen Datenausspäher zur Wehr setzen können und was Sie beachten müssen, wenn Sie einen Strafantrag stellen, erfahren Sie auf den folgenden Seiten.

Datenschutz im Internet

Wenn es um Sicherheit im Internet geht, kommt man am Datenschutz nicht vorbei. Denn **mit jedem Schritt, den Sie im Internet gehen, hinterlassen Sie Datenspuren**. Diese Informationen können gespeichert werden - natürlich nur im Rahmen der gesetzlichen Vorgaben. Dazu gehört beispielsweise das Versenden von E-Mails, der Besuch von Chats und WWW-Seiten sowie der Download von Dateien über FTP und HTTP. Technisch lässt sich das ganz einfach realisieren: Wenn Sie eine Seite anschauen möchten, dann erhält der Webserver, auf dem die Information steht, die **IP-Adresse Ihres Rechners**. Schließlich muss er wissen, an welche Adresse er das angeforderte Dokument senden soll. Beim Aufrufen einer WWW-Seite hinterlassen Sie in den Serverstatistiken der Anbieter persönliche Daten. Der Betreiber kann diese für statistische Zwecke benutzen; er kann aber auch zurück verfolgen, wer Sie sind. Ihre Postanschrift, Ihr Name, Ihre Surfgewohnheiten sind kein Geheimnis, es sei denn, Sie schützen Ihre Daten.

Um den Grundschutz Ihrer Privatsphäre zu gewährleisten, sollten Sie die Einstellungen Ihres Browsers auf Ihre persönlichen Anforderungen anpassen, E-Mails mit vertraulichen Inhalten verschlüsseln und auf eine sichere Übertragung vertraulicher

Daten im Internet - beispielsweise Ihrer Kreditkartennummer beim Online-Shopping - achten. Ist das nicht erkennbar, verzichten Sie besser auf die Weitergabe der Daten. Ein seriöser Anbieter gibt Ihnen immer die Möglichkeit per Nachname oder Rechnung, zu bezahlen.

Weitere Informationen

Sollten Sie sich für den Datenschutz im Internet näher interessieren, haben wir folgende Dokumente für Sie zusammengestellt. Diese und weitere Informationen finden Sie ebenfalls auf der Seite des Bundesbeauftragten für den Datenschutz.

Tätigkeitsbericht 1999 und 2000 des Bundesbeauftragten für den Datenschutz:
tbBfD9900.pdf (4,14 MB)

BfD-INFO 1 - Bundesdatenschutzgesetz - Text und Erläuterung - Diese Broschüre enthält neben dem Gesetzestext und weiteren wichtigen Materialien eine kurze Einführung, die helfen soll, sich die nicht immer einfache Materie zu erschließen. Zugleich eignet sie sich als Basisinformation auch für diejenigen, die beruflich mit personenbezogenen Daten umgehen. Hier finden Sie die 8. Auflage vom April 2002.
info_1.pdf (568 KB)

BfD-INFO 2 - Der Bürger und seine Daten Die Broschüre gibt einen Überblick über die Stellen, die möglicherweise personenbezogene Daten über Bürger erheben, verarbeiten und nutzen und bei denen Sie Ihre Datenschutzrechte geltend machen können. Hier finden Sie die 2. Auflage vom Juli 1999 als PDF-Datei mit der Möglichkeit zum Download.
info_2.pdf (252 KB)

BfD-INFO 3 - Schutz der Sozialdaten Die Broschüre stellt den besonderen Datenschutz im Bereich der Sozialversicherung - also der Kranken-, Unfall- und Rentenversicherung sowie der Arbeitslosen- und der Pflegeversicherung - und auch anderer Sozialleistungen, wie z.B. Sozialhilfe, nach dem Sozialgesetzbuch dar (Stand des Textes November 1994). Die Anhänge 1 und 2 mit den Auszügen aus dem SGB I und SGB X enthalten jeweils einen Link auf die aktualisierten Vorschriften; die Anhänge 3 und 4 verzweigen auf aktuelle Seiten. Hier finden Sie die 1. Auflage vom November 1994 als PDF-Datei mit der Möglichkeit zum Download.
info_3.pdf (296 KB)

BfD-INFO 4 - Der behördliche Datenschutzbeauftragte Die Broschüre informiert über Bestellung, Befugnisse und Aufgaben des behördlichen Datenschutzbeauftragten nach dem alten Bundesdatenschutzgesetz. (2. Auflage von September 1996). Die Neuauflage wird vorbereitet. Hier finden Sie die 2. Auflage vom September 1996 als PDF-Datei mit der Möglichkeit zum Download.
info_4.pdf (81 KB)

BfD-INFO 5 - Datenschutz in der Telekommunikation Die Broschüre gibt einen Überblick über Ihre Datenschutzrechte im Zusammenhang mit der Nutzung von Telekommunikationsdiensten (z. B. Inhalt von Vertragsvordrucken oder Nutzung der

Daten für Werbezwecke). Diejenigen, die beruflich im Bereich der Telekommunikation mit personenbezogenen Daten umgehen, erhalten Hinweise zu einzelnen Rechtsvorschriften. Hier finden Sie die 5. Auflage vom September 2001 als PDF-Datei mit der Möglichkeit zum Download.
info_5.pdf (951 KB)

Internetkriminalität - Hinweise des Bundeskriminalamtes (BKA)

Fast täglich verunsichern Meldungen über Sicherheitslücken und Straftaten im Netz die Internetgemeinde. Die Berichte reichen von massiven finanziellen Schäden durch die so genannten 0190-Dialer über den Computerbetrug oder die Verbreitung von strafrechtlich relevanten Inhalten - dazu zählen beispielsweise Kinderpornographie oder extremistische Äußerungen - bis zur Softwarepiraterie und Computersabotage durch Hacking oder Denial-of-Service-Attacken.

Angesichts seiner überwiegend unbedenklichen Seiten **ist das Internet weit davon entfernt, vorrangig Tummelplatz für Kriminelle zu sein**. In aller Regel kann auch die Datenübertragung über das globale Netz als unbedenklich gelten. **Dennoch gilt es wachsam zu sein:** In dem Maße, wie sich das Internet zum alltäglichen Bestandteil unseres Lebens entwickelt, werden sich auch bekannte Kriminalitätsformen in neuem Gewand in den Datennetzen ausbreiten. Gefahren für den privaten Internetnutzer lauern aber nicht nur bei Betrug oder rechtswidrigen Inhalten, sondern häufig auch bei scheinbar harmlosen Downloads, bei E-Mail-Anhängen oder auf WWW-Seiten mit selbst aktivierenden Inhalten. Und zwar immer dann, wenn Unwissenheit oder Sicherheitslücken mit im Spiel sind.

Was sollten Sie also tun, wenn es Sie trotz aller Vorsichtsmaßnahmen doch einmal erwischt hat und Sie davon ausgehen müssen, Opfer einer Straftat geworden zu sein oder eine solche beobachtet zu haben? Was ist strafbar im Internet, an wen können Sie sich wenden und worauf müssen Sie achten, wenn Sie Anzeige erstatten? **Die folgenden Seiten informieren Sie über die wichtigsten Straftatbestände** im Bereich derjenigen Kriminalitätsformen, die sich gegen das Internet selbst oder seine Inhalte richten - kurz Internetkriminalität genannt.

Strafbare Handlungen im Internet

Viren und Würmer
Das vorsätzliche Versenden / Verbreiten von Viren und Würmern ist in aller Regel als eine versuchte oder vollendete Datenveränderung gem. § 303a StGB strafbar. Problematisch ist dabei allerdings, dass diese Programme aufgrund entsprechender Automatismen oft unwissentlich weiter verbreitet werden. Die fahrlässige oder unwissentliche Verbreitung von Schadprogrammen ist nicht strafbar!

Wird durch den Virus / den Wurm die Computeranlage einer Firma, eines

Unternehmens oder einer Behörde betroffen, kommt darüber hinaus noch eine Strafbarkeit nach § 303b StGB Computersabotage in Frage. Durch ein höheres Strafmaß wird hier der Bedeutung der Datenverarbeitungsanlagen Rechnung getragen.

Anders als zum Beispiel in der Schweiz ist der Besitz von Viren oder das Bereitstellen von Schadprogrammen im Internet nach der derzeitigen deutschen Rechtssprechung ebenfalls nicht strafbar. Beim Bereitstellen könnte allenfalls unter gewissen Umständen der Tatbestand des öffentlichen Aufforderns zu Straftaten erfüllt sein.

IP-Scanning/Port-Scanning
Der Versuch, Zugangsdaten auszuspähen - meist durch IP- bzw. Port-Scanning, gilt als straffrei, wenn der Angriff durch eine Firewall oder ähnliche Programme abgewehrt wird. Dabei ist es für die Bewertung dieses Tatbestandes unerheblich, ob der Rechner im weiteren mit einem Trojanischen Pferd oder anderen Schadprogrammen infiziert wird.

Trojanische Pferde
Häufig kann nicht zweifelsfrei nachgewiesen werden, ob ein Trojanisches Pferd auf dem Opfer-Rechner auch wirklich durch einen eventuell ermittelten Angreifer installiert wurde. Deshalb kommt es bei der Bewertung der Strafbarkeit eher darauf an, was der Täter tatsächlich auf dem Rechner des Opfers angerichtet hat. Bei entsprechenden Täterhandlungen lassen sich dann unter anderem die Straftatbestände der §§ 202a, 303a, 303b StGB subsumieren, wohingegen das bloße Eindringen oder Zugreifen noch nicht strafbar ist.

Um einen Tatverdacht gegen eine bestimmte Person begründen zu können, ist es deshalb notwendig, bei den Geschädigten genauestens abzuklären, wie das Trojanische Pferd auf deren Rechner gelangt sein kann. Eventuell lassen sich verdächtige E-Mails oder auch Internet-Seiten benennen, so dass sich weitere Ermittlungsansätze ergeben. Dabei muss jedoch beachtet werden, dass der Absender nicht unbedingt wissentlich das Trojanische Pferd verbreitet, sondern eventuell selbst Geschädigter ist. Rechtlich umstritten ist, ob bereits beim Installieren eines Trojanischen Pferdes eine rechtswidrige Datenveränderung nach § 303a StGB vorliegt. Als Begründung für das Fehlen eines Straftatbestandes wird angeführt, dass bei jeder Installation eines Programms Programmdateien ohne Einfluss und Kenntnis des Nutzers verändert werden.

DoS-Attacken
Durch DoS-Attacken kann sich der Angreifer in aller Regel wegen rechtswidriger Datenunterdrückung (enthalten im § 303a StGB Datenveränderung) und / oder wegen Computersabotage strafbar machen. Insbesondere bei DDoS-Attacken, bei denen für die Ausführung der Tat andere, gehackte Rechner genutzt werden, kommen weitere Straftaten in Betracht.

Hacking
Im deutschen Strafrecht gibt es den Begriff des Hacking nicht. Allgemein wird darunter jedoch das unberechtigte Eindringen in Computersysteme verstanden. Auch hier ist rechtlich umstritten, ob dabei das bloße Eindringen bereits einen Straftatbestand

darstellt. Erst wenn durch den Hacker auf dem Opfer-System nach dem Eindringen aktiv gehandelt wird, also zum Beispiel Dateien ausgespäht, gelöscht, verändert oder ausgetauscht werden, kann eine Strafbarkeit nach §§ 202a oder 303a, 303b StGB gegeben sein.

Bei Unternehmen kommt darüber hinaus noch § 17 UWG in Betracht, da nicht auszuschließen ist, dass in die Rechner eingedrungen wird, um Daten mit geschäftlichem Hintergrund auszuspähen oder zu erlangen. Der Besitz und das Anbieten von Hackertools (rootkits o.ä.) sind derzeit in Deutschland in aller Regel nicht strafbar, wohl aber in einigen anderen europäischen Ländern.

Unberechtigtes Nutzen von Zugangsdaten
Das unberechtigte Nutzen von Zugangsdaten zum Internet ist insbesondere für die Geschädigten, in der Regel Privatpersonen, ein ärgerliches Vorkommnis, da im Gegensatz zu den vorher aufgeführten Delikten hier direkt der eigene Geldbeutel betroffen ist. Oft kursieren die ausgespähten Zugangsdaten bereits kurze Zeit später im Internet. Deshalb gibt es meistens eine Vielzahl von Tätern, die auf Kosten eines Geschädigten surfen. Derjenige, der die Daten - meistens durch den Einsatz eines Trojanischen Pferdes - erlangt hat, macht sich wegen Ausspähens von Daten gemäß § 202a StGB sowie möglicherweise wegen Datenveränderung gemäß § 303a StGB strafbar. Diejenigen, die diese Daten dann einsetzen, handeln rechtswidrig wegen Computerbetrug gemäß § 263a StGB.

0190-Dialer
Insbesondere durch die missbräuchliche Verwendung von Einwahlprogrammen, den so genannten 0190-Dialern, entwickeln sich diese zu einer wahren Kostenfalle und können erhebliche finanzielle Schäden verursachen. Die meisten der verwendeten Dialer sind so geartet, dass ein Verstoß gegen bestehende Rechtsnormen nicht erkennbar ist. Zur Kategorie "strafrechtlich bedeutsam" gehören aber Dialer,

- die keine Tarifangabe vor oder während der Installation bzw. vor der Einwahl anzeigen.
- die eine falsche Tarifangabe anzeigen.
- die sich unbemerkt im Hintergrund (ggf. als Standardverbindung auch für zukünftige Anwahlen) installieren, ohne dafür eine Bestätigung vom Nutzer per Mausklick zu benötigen.

Häufig werden auch solche Dialer, die an sich strafrechtlich nicht relevant sind, genutzt, um Produkte zu veräußern, die sich am Rande oder außerhalb der Legalität bewegen. Beispiele hierfür sind:

- Der Vertrieb von raubkopierten Filmen und raubkopierter Software (Link zu Softwarepiraterie).
- Der Vertrieb von "Hackertools" (Hilfsprogramme zum Ausspähen von Daten, Programmieren von Viren, Entschlüsseln von PayTV-Sendern, E-Mail-Bombing etc.).

Durch diverse "Maschen" oder zweifelhafte Angebote wird versucht, die Internetnutzer zum Herunterladen und zur Installation des 0190er-Dialerprogramms zu bewegen. Hier einige Beispiele:

- Es wird versprochen, dass nach dem Download dieses Programms eine schnellere Übertragungsrate beim Surfen im Internet möglich ist (sog. "Highspeed-Internetzugang").
- Der Dialer wird als "kostenlose Zugangssoftware" bezeichnet. Diese sei notwendig zum Besichtigen der gewünschten Seite.
- Es wird behauptet, dass dieser Dialer "gecrackt" sei und somit keine Kosten verursache.
- Es werden bekannte Programmnamen benutzt.
- Benutzung einer Vorwahl vor der Service 0190-Nummer, um damit die inzwischen verbreiteten "Service 0190-Warner" auszutricksen und den Charakter der Nummer zu verschleiern.
- Es werden angebliche Sicherheitsprobleme des Computers mit simplen HTML-Tricks angezeigt. Anschließend erscheint ein Angebot zum Download von Schutzprogrammen, die dann nur über den Dialer zu erreichen sind.

Besonders die so genannten "cracked-Dialer" sind in letzter Zeit häufig Gegenstand von Anfragen besorgter Bürger bei der Polizei. Zum einen ist die Frage, ob diese Dialer tatsächlich einen kostenlosen Zugang auf kostenpflichtige Seiten ermöglichen, zum anderen erstatten die Bürger Anzeige gegen das in ihren Augen strafrechtlich relevante Verhalten der Anbieter. Nach hiesiger Meinung gibt es keine Dialer, die einen kostenlosen Zugang auf ansonsten kostenpflichtige Seiten ermöglichen. Erfahrungsgemäß steht im Infofenster des Dialers sogar der reale Betrag, der nach Einwahl fällig wird. Teilweise ist der Dialer verfälscht, indem das Infofenster so manipuliert wurde, dass ein Preis pro Minute von 0,00 Euro angezeigt wird. Berechnet wird hingegen der normale Betrag, abhängig von der jeweiligen 0190-Einwahlnummer.

Im Internet gibt es mittlerweile mehrere Seiten, die sich mit den Problemen im Zusammenhang mit 0190er-Dialern beschäftigen:

- www.dialerschutz.de/
- www.trojaner-info.de/
- www.dialerundrecht.de/
- www.dialerhilfe.de/
- www.bsi.bund.de/
- www.regtp.de/
- www.fst-ev.de/
- www.propk.de/

Auf diesen Seiten können sich Nutzer über rechtliche Entwicklungen, neue Begehungsweisen der Betrüger oder über Verhaltensweisen nach "Infizierung" mit einem Dialer informieren. So plant die Bundesregierung für 2003 wesentliche Veränderungen, um den Missbrauche von Mehrwertdienst-Rufnummern zu verhindern. Zudem besteht die Möglichkeit des Herunterladens von Softwaretools beziehungsweise 0190-Warnern.

Grundsätzlich in Frage kommende Straftatbestände wären § 303a Datenveränderung und/oder § 263a StGB Computerbetrug. Eine Strafbarkeit kann nur im Einzelfall geprüft werden; diese Prüfung ist nur möglich, wenn den Strafverfolgungsbehörden alle

erforderlichen Informationen zur Verfügung gestellt werden. Hier gilt es Regeln der Beweissicherung zu beachten (siehe Kapitel Abzocker & Spione). Im Einzelfall ist es sinnvoll, wenn die Festplatte oder auch der gesamte Computer des Geschädigten mit dem noch installierten Dialer zur Auswertung übergeben wird.

Handel im Internet E-Commerce ist auf dem Vormarsch und mittlerweile ein fester Bestandteil des Internet. Wo angeboten und gekauft wird, ist zwangsläufig auch Betrug nicht weit. Im Strafrecht ist hier vor allem § 263a Computerbetrug relevant. Auf den Seiten des Programms der polizeilichen Kriminalprävention (www.polizei.propk.de/) finden sie Hinweise, welche Gefahren es gibt und wie Sie sich schützen können.

Kinder- und Jugendschutz Zunehmend wird es wichtig, dass sich auch Kinder und Jugendliche frühzeitig mit der Cyber-Welt vertraut machen. Wie in allen anonymen Medien hat sich allerdings leider auch im World Wide Web ein Markt für Sex und Gewalt gebildet. Hier finden Sie wiederum auf den Seiten des ProPK (www.polizei.propk.de/) Tipps, die Ihnen helfen, Ihren Nachwuchs vor "Rotlichtbezirken" und gewaltverherrlichenden Seiten im Netz zu schützen. Die meisten Landeskriminalämter haben zudem eigene Links (siehe Links zur Polizei im Internet) eingerichtet, über die Sie im Falle eines Falles Hinweise auf strafbare Inhalte im Netz geben und ggf. Anzeige erstatten können.

Softwarepiraterie/Kostenlose Zugänge zu Zahlungspflichtigen Angeboten Im Verlauf der letzten Jahre ist in Deutschland ein Markt für den entgeltlichen Abruf von Fernsehprogrammen, Online-Informationen und sonstigen Informations- und Kommunikationsdiensten entstanden. Solche Dienste sind nur dann rentabel, wenn sie durch Zugangskontrollen vor unbefugtem Empfang geschützt sind. Damit soll gewährleistet werden, dass der Nutzer für den jeweiligen Abruf eines Dienstes das dafür vorgesehene Entgelt entrichtet.

In der Praxis werden allerdings Geräte, Computersysteme und Computerprogramme vertrieben, mit denen geschützte Rundfunk- und Internetdienste ohne die Genehmigung des Diensteanbieters empfangen werden können. Durch diese "Piraterie" entstehen den Anbietern von so genannten zugangskontrollierten Diensten (z.B. Pay-TV, Video-on-demand, passwortgeschützte Internetdienste, entgeltliche Computerspiele, bei denen mehrere Teilnehmer über das Internet miteinander spielen) erhebliche finanzielle Schäden. Um diesem Phänomen entgegenzuwirken, trat am 23. März 2002 das Gesetz über den Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten (ZKDSG) in Kraft, das unerlaubte gewerbsmäßige Maßnahmen zur Umgehung von Schutzvorrichtungen und bestimmte Unterstützungshandlungen verbietet. So verbietet das Gesetz in **§ 3 Nr. 1** zunächst die Herstellung, Einfuhr und Verbreitung von sog. **Umgehungsvorrichtungen** - also den Geräten, die unbefugten Empfang von zugangskontrollierten Diensten ermöglichen, wie zum Beispiel manche Software, nicht autorisierte Decoder, Smartcards oder Programme, mit denen Passwörter oder sonstige Autorisierungscodes geknackt werden - zu gewerbsmäßigen Zwecken. Bewusst wurde hier, wie auch in der folgenden Verbotsvorschrift, lediglich das Handeln zu **gewerbsmäßigen Zwecken** - das heißt jede nachhaltige Tätigkeit zur Erzielung von Einnahmen, auch wenn die Absicht, Gewinn zu erzielen, fehlt - verboten.

Bei **nicht gewerbsmäßigem** Verhalten kommt eine Strafbarkeit nach den §§ 265a (Erschleichen von Leistungen - auch die Leistung eines Decodersystems zur Nutzung verschlüsselter TV-Programme ist als Automatenleistung i.S.d. Norm zu sehen), 263a (Computerbetrug) oder 202a (Ausspähen von Daten) StGB in Betracht. Ein **Verstoß gegen § 3 Nr. 1 ZKGSD** wird gem. § 4 mit **Freiheitsstrafe** bis zu einem Jahr bestraft. Außerdem können gem. **§ 6** Gegenstände, auf die sich eine solche Straftat bezieht (so genannte **Beziehungsgegenstände**) **eingezogen** werden. Dies bedeutet zum Beispiel für den Fall, in dem der Täter gem. § 3 Nr. 1 ZKGSD verbotenerweise Umgehungsvorrichtungen gewerbsmäßig hergestellt hat, dass die Umgehungsvorrichtung aus dem Verkehr gezogen werden kann. Darüber hinaus droht gem. § 74 StGB die **Einziehung des Tatwerkzeuges** (zum Beispiel des Computers, mit dem die Crackersoftware erstellt wurde) oder **der Produkte der Tat** (zum Beispiel unerlaubt heruntergeladene Videos). Natürlich drohen auch **zivilrechtliche Ansprüche** (z.B. nach §§ 812, 823 II BGB).

Ferner ist der Besitz, die technische Einrichtung, die Wartung und der Austausch von Umgehungsvorrichtungen zu gewerbsmäßigen Zwecken gem. **§ 3 Nr. 2 ZKGSD** verboten. Auch hier ist der gewerbsmäßige Zweck Voraussetzung für jeden der aufgezählten Fälle. Der nichtgewerbsmäßige Besitz durch private "Schwarznutzer" und Cracker ist nach diesem Gesetz nicht verboten (evtl. aber gem. §§ 202a, 263a, 265a StGB). Wer gegen **§ 3 Nr. 2 ZKDSG** verstößt, handelt ordnungswidrig und kann mit einer Geldbuße bis zu 50.000 Euro belangt werden.

Gemäß **§ 3 Nr. 3 ZKGSD** schließlich ist auch die **Absatzförderung** - das heißt alle auch nicht gewerbsmäßig vorgenommenen Absatzförderungsmaßnahmen - von Umgehungsvorrich-tungen verboten. Hierunter fällt zum Beispiel das Ins-Netz-stellen von Crack-Software zum kostenlosen Download. Ein Verstoß gegen § 3 Nr. 3 ZKGSD ist weder bußgeldbewehrt noch wird er mit Strafe geahndet. Allerdings können sich hieraus Möglichkeiten zum präventiven Vorgehen der Polizei auf der Grundlage der Landespolizeigesetze oder zivilrechtliche Ansprüche der Diensteanbieter ergeben (das ZKDSG ist Schutzgesetz i.S.d. 823 II BGB).

Straftatbestände - die wichtigsten Paragraphen des StGB und des UWG mit Bezug zur Internetkriminalität

Strafgesetzbuch

§ 202a - Ausspähen von Daten

(1) Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden

§ 205 - Strafantrag

(1) In den Fällen des ...und der §§ 202 bis 204 wird die Tat nur auf Antrag verfolgt.

§ 263a - Computerbetrug

(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, dass er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

§ 265a - Erschleichen von Leistungen

(1) Wer die Leistung eines Automaten oder eines öffentlichen Zwecken dienenden Telekommunikationsnetzes, die Beförderung durch ein Verkehrsmittel oder den Zutritt zu einer Veranstaltung oder einer Einrichtung in der Absicht erschleicht, das Entgelt nicht zu entrichten, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

(2) Der Versuch ist strafbar.

§ 303a - Datenveränderung

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

§ 303b Computersabotage

(1) Wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, dass er 1. eine Tat nach § 303a Abs. 1 begeht oder 2. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

§ 303c - Strafantrag

In den Fällen der §§ 303 bis 303b wird die Tat nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

UWG - Gesetz gegen den unlauteren Wettbewerb
§ 17 - Verrat von Geschäfts- oder Betriebsgeheimnissen

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer als Angestellter, Arbeiter oder Lehrling eines Geschäftsbetriebs ein Geschäfts- oder Betriebsgeheimnis, das ihm vermöge des Dienstverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Dienstverhältnisses unbefugt an jemand zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Geschäftsbetriebs Schaden zuzufügen, mitteilt.

(2) Ebenso wird bestraft, wer zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Geschäftsbetriebs Schaden zuzufügen, 1. sich ein Geschäfts- oder Betriebsgeheimnis durch a) Anwendung technischer Mittel, b) Herstellung einer verkörperten Wiedergabe des Geheimnisses oder c) Wegnahme einer Sache, in der das Geheimnis verkörpert ist, unbefugt verschafft oder sichert oder 2. ein Geschäfts- oder Betriebsgeheimnis, das er durch eine der in Absatz 1 bezeichneten Mitteilungen oder durch eine eigene oder fremde Handlung nach Nummer 1 erlangt oder sich sonst unbefugt verschafft oder gesichert hat, unbefugt verwertet oder jemandem mitteilt.

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter bei der Mitteilung weiß, dass das Geheimnis im Ausland verwertet werden soll, oder wenn er es selbst im Ausland verwertet.

An wen Sie sich wenden können und worauf Sie bei einer Anzeige achten sollten

Strafanzeige
Eine Strafanzeige ist genau genommen jede Mitteilung an eine Strafverfolgungsbehörde über eine Straftat. Strafanzeigen können bei Staatsanwaltschaft, Polizeidienststellen oder -beamten und den Amtsgerichten mündlich oder schriftlich erstattet werden. Einige Straftaten, wie zum Beispiel §§ 202a, 303a und 303b StGB können jedoch nur auf Antrag verfolgt werden (siehe unter Strafantrag). Im Ausland sind in der Regel die deutschen Botschaften beim Kontakt mit den dortigen Strafverfolgungsbehörden behilflich.

Achten Sie bei schriftlichen Anzeigen darauf, Ihre persönliche Erreichbarkeit (Anschrift, Telefon, E-Mail etc.) anzugeben und möglichst genaue Angaben zum (wahrscheinlichen) Tatzeitpunkt, zu den Schäden und zu Ihren weiteren Beobachtungen zu machen.

Strafantrag
Strafantrag kann nur durch den Geschädigten oder eine andere berechtigte Person

gestellt werden. Es empfiehlt sich daher, bei Anzeigenerstattung als Geschädigter an die Polizei grundsätzlich die Formulierung

"Ich stelle Strafantrag aus allen rechtlichen Gründen."

zu verwenden. So ist gewährleistet, dass die Strafverfolgung nicht wegen des fehlenden Antrages eingestellt wird.

Nachfolgend die gesetzlichen Vorschriften zum Strafantrag:
§ 77 StGB - Antragsberechtigte

(1) Ist die Tat nur auf Antrag verfolgbar, so kann, soweit das Gesetz nichts anderes bestimmt, der Verletzte den Antrag stellen.

§ 77b StGB - Antragsfrist

(1) Eine Tat, die nur auf Antrag verfolgbar ist, wird nicht verfolgt, wenn der Antragsberechtigte es unterlässt, den Antrag bis zum Ablauf einer Frist von drei Monaten zu stellen.

(2) Die Frist beginnt mit Ablauf des Tages, an dem der Berechtigte von der Tat und der Person des Täters Kenntnis erlangt.

§ 77d StGB - Zurücknahme des Antrags

(1) Der Antrag kann zurückgenommen werden. Die Zurücknahme kann bis zum rechtskräftigen Abschluss des Strafverfahrens erklärt werden. Ein zurückgenommener Antrag kann nicht nochmals gestellt werden.

Die Strafanzeige bzw. das Verfahren wird im weiteren, entsprechend der gesetzlichen Vorschriften, an die jeweilig zuständige Behörde abgegeben. Die Zuständigkeit richtet sich hierbei nach unterschiedlichen Kriterien, die im Fall von Internetkriminalität nicht immer eindeutig sind.

Normalerweise gilt der Grundsatz, dass das Verfahren am Wohnsitz des Tatverdächtigen geführt wird. Da insbesondere im Bereich der Computerkriminalität in den seltensten Fällen am Anfang der Ermittlungen bereits ein Tatverdächtiger namentlich bekannt ist, wird das Ermittlungsverfahren dann am Schadensort (zum Beispiel Wohnsitz des Geschädigten, Serverstandort der Firma) geführt.

Es empfiehlt sich daher, im Schadensfall zu **seiner örtlich zuständigen Polizeidienststelle** zu gehen, damit man vor Ort alle notwendigen Unterlagen oder Daten (E-Mail mit Virus auf Diskette usw.) übergeben und gleichzeitig im direkten Kontakt mögliche Fragen klären kann.

Firmen, die sich aufgrund ihrer Geschäftstätigkeit oder wirtschaftlichen Bedeutung einer gewissen Bedrohung ihrer EDV-Anlagen ausgesetzt sehen, sollten bereits im Vorfeld Kontakt zu den für Computerkriminalität zuständigen polizeilichen Sachbearbeitern

aufnehmen, um kurzfristig reagieren zu können.

Beweismittel
Generell sollte alles, was für die Ermittlungen von Bedeutung sein könnte, an die Strafverfolgungsbehörden übergeben werden. Hierzu können **Korrespondenzen mit dem Täter, erhaltene E-Mails mit Anhängen, Logfiles des geschädigten Systems** u.ä. zählen.

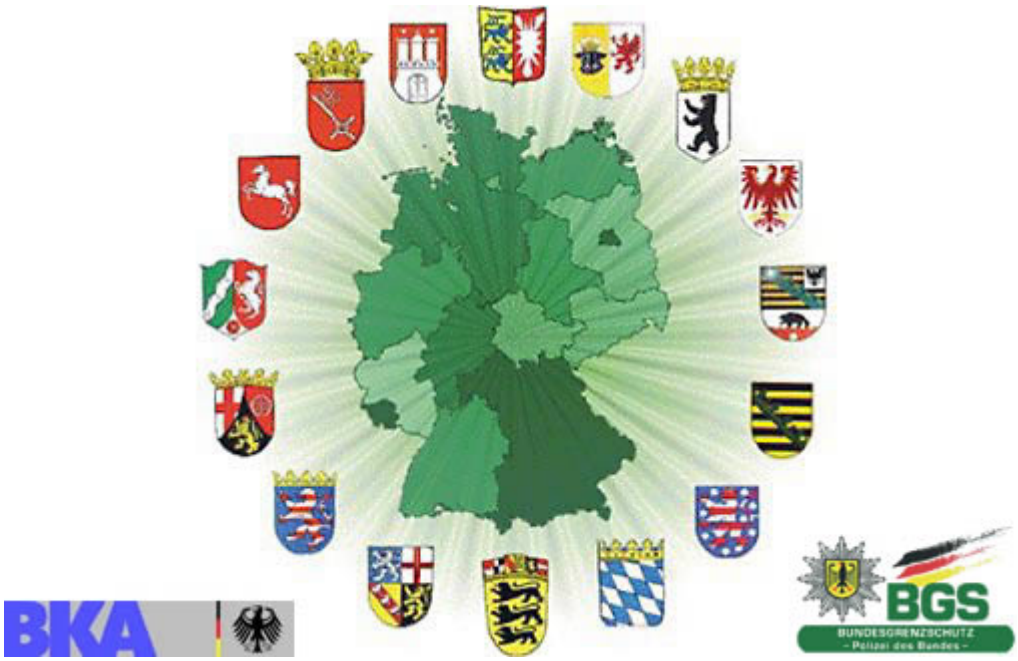
Wichtig ist, dass - soweit möglich - alle Beweismittel im Originalzustand, das heißt auf den betroffenen Datenträgern (mindestens als Kopie) oder bei gehackten Rechnern und 0190-Dialern möglichst komplette Datensätze (ggf. also die gesamte Festplatte oder sogar der Rechner) übergeben werden. Nur so können ausreichende Ermittlungsansätze gewonnen werden, die eine effektive Auswertung ermöglichen.

Wenn die E-Mail, an der sich als Anlage ein unbekannter Virus befunden haben soll, nur in ausgedruckter Form vorliegt, können daraus kaum Ermittlungsansätze gewonnen werden. Denn häufig fehlt der komplette Kopfbereich der E-Mail (Header) und zum anderen ist die Beweiskraft natürlich deutlich höher, wenn der Virus tatsächlich vorhanden und gesichert ist.

Ebenso ist es bei 0190-Dialern unmöglich, bei bereits gelöschten Daten oder sogar neu formatierten Rechnern entsprechende Beweismittel über die Funktionsweise der Dialer nachzuvollziehen. Gerade diese Fakten sind aber hinsichtlich Aussagen über eine eventuelle Strafbarkeit unerlässlich.

Links zur Polizei im Internet

Das Vorbeugeprogramm der Polizei: www.polizei.propk.de/



Polizei Schleswig-Holstein	www.polizei.schleswig-holstein.de
Polizei Mecklenburg-Vorpommern	www.polizei.mvnet.de/
Polizei Berlin	www.polizei.berlin.de
Polizei Brandenburg	www.polizei.brandenburg.de/
Polizei Sachsen-Anhalt	www.polizei.sachsen-anhalt.de
Polizei Sachsen	www.polizei.sachsen.de
Polizei Thüringen	www.polizei.thueringen.de
Polizei Bayern	www.polizei.bayern.de/
Polizei Baden-Württemberg	www.polizei-bw.de
Polizei Saarland	www.polizei.saarland.de
Polizei Hessen	www.polizei.hessen.de
Polizei Rheinland-Pfalz	www.polizei.rpl.de
Polizei Nordrhein-Westfalen	www.polizei.nrw.de
Polizei Niedersachsen	www.polizei.niedersachsen.de
Polizei Bremen	www.polizei.bremen.de
Polizei Hamburg	www.polizei.hamburg.de
Bundeskriminalamt	www.bka.de/
Bundesgrenzschutz	www.bundesgrenzschutz.de/