Internet transparent

**Ergänzung zum gleichnamigen Artikel aus PCNEWS-58, Seite 66.
Auch als WIFI-Skriptum erschienen.**

Christian Zahler

Inhaltsverzeichnis

1 Suchen und Finden im Internet

Das Internet ist chaotisch organisiert. Nutzer bekommen unkontrolliert den Zugang zum Web, jeder kann seine Meinung kundtun, jeder kann eine Homepage veröffentlichen. Dadurch kann das Internet rasch wachsen und dadurch kommen auch sehr rasch Informationen ins Netz. Die ganze Welt ist aus einem "Chaos" entstanden - offensichtlich die beste Entwicklungsstrategie. So ist es auch mit dem Internet zu verstehen. Diese chaotische Entwicklung birgt ein großes Entwicklungspotential mit sich und ist daher durchaus positiv zu sehen.

Im Internet sind bereits (Stand Anfang 2000) um die (geschätzten) 1 Milliarde Informationsseiten vorhanden. Wenn man bedenkt, dass diese Menge erst seit 1994 entstanden ist, so ist das ein gewaltiges Wachstum. Noch nie vorher hat eine Technologie so schnell Verbreitung und Akzeptanz gefunden.

Ein Internet-Anschluss alleine genügt nicht. Der Mensch muss lernen, mit dieser neuen Kulturtechnik umzugehen und umzudenken von "Ich muss alles wissen" auf "Ich weiß es zu finden". So ist er in der Lage, das im Internet verfügbare "Wissen der Welt" auch für sich gewinnbringend zu nutzen.

Die Internetdokumente liegen auf vielen Millionen Rechnern verteilt. Um in diesem Chaos etwas finden zu können, haben sich Suchmaschinen ("Search-Engines") etabliert. Diese kostenlos nutzbaren Dienste haben aus dem kostenlosen Service ein großes Geschäft gemacht. Sie werden täglich viele Millionen Mal kontaktiert und können so Werbung an den Mann/an die Frau bringen. Für diese Werbeeinschaltungen bekommen die Suchmaschinenbetreiber viel Geld.

Man unterscheidet "echte" Suchmaschinen und sogenannte "Kataloge". Suchmaschinen arbeiten meist vollautomatisch, während Kataloge oft redaktionell betreut werden. Die gemeldeten Seiten werden von Menschen durchgesehen und Kategorien zugewiesen.

Wie arbeitet eine Suchmaschine?

Eine Suchmaschine sucht nicht selber (zum Abfragezeitpunkt) nach Informationen. Mit dieser Methode könnte sie nie rasch genug ein Suchergebnis anbieten. Es wird ein großer - lokaler - Index durchsucht. Da Suchmaschinen auf sehr leistungsfähigen Rechnern laufen, dauert die Antwort oft nur wenige Sekunden. Die Bedienung der Suchmaschinen ist im wesentlichen gleich: Man gibt in ein - aus einem Feld bestehenden - Formular ein oder mehrere Suchbegriffe ein, klickt auf den "Absendeknopf" (meist neben dem Feld befindlich). Das Suchergebnis wird in Form einer "Linkliste" (Link: die "Verbindung" zu einer weiteren Seite) präsentiert - meist in "Portionen" zu 10 "Treffern". Am Ende der Linkliste gibt es meist eine Leiste/Texte oder "Knöpfe", über die man die Folgeseiten erreicht. Die Links kann man anklicken und bekommt dann die entsprechenden "Originalseiten" vom "Originalserver" (also nicht mehr von der Suchmaschine) präsentiert.

Meist findet die Suchmaschine mehrere tausend oder hunderttausend Seiten. Stellen sich die Fragen: Welche davon ist für mich interessant? Muss ich jetzt alle Links durchsehen?

Meist sind die ersten 2-4 Seiten (20-40 Links) die interessantesten. Wieso? Die Suchmaschine nimmt eine Rangordnung vor und reiht die Ergebnisse nach Relevanz. Wenn man also unter den ersten 40 Links nichts Passendes gefunden hat, versucht man die Abfrage mit anderen bzw. zusätzlichen Suchworten. Die Recherche im Internet ist grundsätzlich eine einfache Sache, doch benötigt man etwas Geschick und Übung, damit man rascher an den "Kern" der Sache kommt.

Um ein bestimmtes Thema auszurecherchieren sollte man schon einige Zeit einplanen. Während der Recherche lernt man laufend dazu, findet neue Suchbegriffe, die man für eine neue Suche verwenden wird. Am Ende der Recherche ist man ein echter Spezialist für dieses Thema geworden.

Es gibt viele deutsche Informationsseiten (Homepages) im Internet, jedoch noch mehr englischsprachige. Suchen Sie in mehreren Suchmaschinen - auch in englischsprachigen und in englischsprachigen Dokumenten.

Bei Suchmaschinen ist grundsätzlich (fast) jedes Wort, das auf einer Homepage steht, ein möglicher Suchbegriff.

Meta-Such-Maschinen / Crawler:

Diese Suchmaschinen haben keinen eigenen Index, sondern geben Suchanfragen parallel an eine Reihe von Suchmaschinen weiter, Die empfangenen Ergebnisse werden verdichtet, nach Relevanz gereiht und präsentiert.

Kataloge

Kataloge sind nach Kategorien gegliederte Inhaltsverzeichnisse. Man klickt sich durch die Themen durch oder gibt Stichworte ein. Kataloge sind keine "Suchmaschinen" und nehmen nicht jedes Wort einer Homepage als Suchbegriff auf. Da die angemeldeten Seiten jedoch "redaktionell" von Menschen durchgesehen werden, ist deren Qualität sehr gut. Kataloge haben meist wesentlich weniger angemeldete Seiten.

Das Suchen / Tipps und Tricks

- Geben Sie ein oder mehrere Suchbegriffe ein
- Trennen Sie die Suchbegriffe durch Leerstellen
- Schreiben Sie alle Suchbegriffe klein!
- Achten Sie auf die Internet-Adresse in der URL-Zeile. Wenn Sie eine Homepage suchen, dann kann der Domain-Name weiterhelfen!
- Wenn Sie auf einer Unterseite einer Homepage sind, dann können Sie den Text nach dem Domainnamen in der URL-Zeile weglöschen, dann sollten Sie auf die Einstiegsseite kommen.
- Variieren Sie die Suchbegriffe. Wenn Sie noch nichts Passendes gefunden haben, dann haben Sie noch nicht "optimal" gesucht.
- Lernen Sie bei jeder Suchabfrage dazu und gehen Sie wieder suchen
- Verwenden Sie mehrere Suchmaschinen, Nicht jede Suchmaschine hat die gleichen Seiten im Index!
- "..." halten mehrere Worte wie einen Suchbegriff zusammen
- + direkt vor einem Suchbegriff bedeutet "genau dieses Wort muss auf der Seite vorkommen"
- Suchwort ohne "+" davor: Es werden Seiten gefunden, wo dieses Wort vorkommt, aber auch zusammengesetzte Worte, die so beginnen.
- Achten Sie auf die Trefferanzahl und experimentieren Sie mit den Suchbegriffen und Möglichkeiten. Anhand der Anzahl der gefunden Web-Seiten sehen Sie die Auswirkungen Ihrer Abfragevarianten.
- In der "Profi-Suche" kann man logische Verknüpfungsworte wie "and", "or", "and near", "and not" verwenden. Setzen Sie Klammern, um die logischen Prioritäten

zu ändern! (z.B.: "gebrauchtwagen and (porsche 911 or ferrari")

- Suchen Sie auch nach Datenbanken. Angebote in Datenbanken sind vor Suchmaschinen "versteckt". (Suchen Sie in diesem Fall nach z.B.: "gebrauchtwagen datenbank").
- Sie finden Näheres unter "Hilfe" oder "help" bei den einzelnen Suchmaschinen!

Suchmaschinen

Altavista: http://www.altavista.de/

Große Suchmaschine mit deutschsprachiger Benutzeroberfläche

Altavista: http://www.altavista.com/

Die "Mutter" der deutschsprachigen Tochter, Millionen von Dokumenten.

Austronaut: http://www.austronaut.at/

Österreichische Suchmaschine

Fireball: http://www.fireball.de/

Große deutsche Suchmaschine

Meta-Suchmaschine

Metager: http://www.metager.de/

... und weitere 2000 Suchmaschinen.

Suchmaschinen & Such-Know-How

http://www.schnellsuche.de/

Suchen Sie nach Suchmaschinen mit den Suchbegriffen:

search engine

search engines

search engines index

Kataloge

YAHOO

http://www.yahoo.de/
http://www.yahoo.com/

(größter und ältester Katalog)

Klammeraffe

http://www.klammeraffe.at/

Übungen

- Suchen sie über die Suchmaschine Austronaut http://www.austronaut.at/ die Homepage der Volksanwaltschaft in Österreich

Wie kommen die Seiten in eine Suchmaschine / Katalog?

Suchmaschinen nehmen dann Homepages in ihren Index auf, wenn sie dort angemeldet werden. Nur ein paar Suchmaschinen streifen selbständig durchs Web und holen sich die Seiten selber. Daher: Wenn man gefunden werden will, muss man seine Homepage (mit der URL) dort anmelden. Nach der Anmeldung dauert es zwischen 2 Tagen und 2 Monaten (ist abhängig von der Suchmaschine), bis man wirklich gefunden wird.

Man findet das Eintragsformular meist unter Links wie

- Seite anmelden
- URL eintragen
- Seite eintragen
- Add URL
- u.s.w.

Tragen Sie Ihre Homepage in möglichst vielen Suchmaschinen und Katalogen ein. Ein "Submit Service" kann Ihnen da - meist gegen eine Gebühr - behilflich sein. Links zu Submit-Services finden Sie bei den Suchmaschinen oder Sie suchen sie mit den Suchbegriffen "Submit Service" oder "Submit Services"

Näheres finden Sie wieder auf den Seiten der Suchmaschinen (z.B.: Hilfe, Help, Info, FAQ)

(Übrigens: das sollten Sie kennen: **URL**: *Uniform Ressource Locator* und ist die Internet-Adresse, die Sie auch im Browser eingeben. **FAQ**: Frequently Asked Questions = häufig gestellte Fragen)

2 Technische Grundlagen des Internets

Jedes Netzwerk braucht Gemeinsamkeiten. Die (einzige!) Gemeinsamkeit im Internet ist die Art der Datenübertragung, das so genannte Protokoll. Im Internet wird das so genannte TCP/IP (*Transfer Control Protocol/Internet Protocol*) verwendet.

Jeder Rechner auf der ganzen Welt braucht eine eindeutige Adresse, um im Internet erkannt zu werden, die so genannte IP-Adresse. (Diese Adresse wird vom *Internet Protocol* IP genutzt). In der derzeit gültigen Version 4 des Internet Protokolls ist die IP-Adresse eine 32-stellige Binärzahl, also etwa:

1011001.01010011.11001111.00010001

Meist fasst man 8 Binärstellen (bits) zu einem Byte zusammen, dessen Wert man berechnet. Die "Kurzschreibweise" der oben angeführten IP-Adresse würde daher zum Beispiel lauten:

217.83.207.17

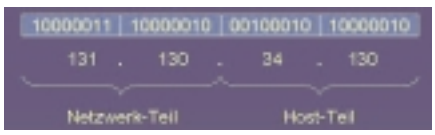
Diese Adressen werden von der *Internet Number Association* (IANE) vergeben.

Man hat also mit einer solchen 32 bit-Adresse insgesamt 232 = 4 294 967 296 Möglichkeiten (also mehr als 4 Milliarden), einen PC unverwechselbar zu adressieren. Man sollte meinen, dass diese große Anzahl für alle PCs der Welt ausreicht. Leider ist das nicht so!

Diese Adressen sind nämlich in zwei Teile geteilt:

Der erste Teil ist die **Netzwerk-Adresse**. Da das Internet aus vielen miteinander verbundenen lokalen Netzen (LAN) besteht, ist es sinnvoll, jedem LAN eine eindeutige Adresse zuzuweisen.

Der zweite Teil gibt die Adresse der einzelnen Rechner im Netz an (**Host-Adresse**). Dieser Teil wird durch das lokale Netzwerkmanagement frei vergeben.



Man hat nun verschiedene Größenklassen von Netzwerken festgelegt:

Class-A-Netze: Adresse beginnt mit einer binären 0, 7 bit für Netzwerk-Adresse, 24 bit für Host-Adresse. Damit gibt es weltweit 127 derartige Netzwerke, ein Class-A-Netz kann bis zu 16 Mio. Teilnehmer haben. Alle derartigen Netzadressen sind bereits belegt.

IP-Adressen von Class-A-Netzen:

0.0.0.0 bis 127.255.255.255

Class-B-Netze: Adresse beginnt mit der binären Ziffernkombination 10, 14 bit für Netzwerk-Adresse, 16 bit für Host-Adresse. Damit gibt es weltweit 16384 derartige Netzwerke, ein Class-B-Netz kann bis zu 65536 Teilnehmer haben. Alle derartigen Netzadressen sind bereits belegt.

IP-Adressen von Class-B-Netzen:

128.0.0.0bis 191.255.255.255

Class-C-Netze: Adresse beginnt mit der binären Ziffernkombination 110, 21 bit für Netzwerk-Adresse, 8 bit für Host-Adresse. Damit gibt es weltweit 2 Milliomen derartige Netzwerke, ein Class-C-Netz kann bis zu 256 Teilnehmer haben. Neu zugeteilte Netzadressen sind heute immer vom Typ C. Es ist abzusehen, dass bereits in Kürze alle derartigen Adressen vergeben sein werden. Man arbeitet daher an einem neuen Standard (Version 6 des Internet Protokolls, **IPv6** oder **IPng** für "*new generation*"), der statt einer Adresslänge von 32 bit eine Länge von 128 bit haben soll. Um die Kompatibilität zu gewährleisten, wird die alte Adresse in der neuen Adresse "enthalten sein".

IP-Adressen von Class-C-Netzen:

192.0.0.0 bis 223.255.255.255

Class D-Netze haben einen speziellen Anwendungsbereich (Multicast-Anwendungen) und haben für Internet keine Bedeutung.

Laut RFC 1918 sind für "**private**" **Netze folgende IP-Bereiche** gestattet (Rechner mit diesen IP-Adressen dürfen keinen direkten Internet-Verkehr haben, d.h. mit dem Internet nur über Proxy-Server in Kontakt treten; sie werden nicht geroutet!):

10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

Für einen Anwender sind derartige Zahlenkombinationen schwer zu merken. Es werden daher statt dieser Zahlendarstellung symbolische Namen verwendet.

So gibt es etwa einen Server mit dem Namen

noe.wifi.at

Diesem Servernamen entspricht eine eindeutige IP-Adresse. Dabei setzt sich der Name aus Teilen zusammen, die eine Hierarchie angeben: Das Teilnetzwerk "**noe**" (fachchinesisch bezeichnet man ein solches Teilnetz als **Domäne**, englisch *domain*) ist ein Teil des Netzwerks "**wifi**", dieses wiederum ein Teil des Netzwerks "**at**" (für Österreich). Das "**at**"-Netzwerk ist ein Teil der Domäne "the world" (die aber nie angegeben zu werden braucht).

Die Länderkennung ist ein Beispiel für eine *Top Level Domain* (TLD); so werden

die "Haupt-Domänen" bezeichnet, die entweder einem Land oder einer "Kategorie" entsprechen.

Die Zuordnung IP-Adressen zu logischen Namen muss von einem eigenen Rechner durchgeführt werden, dem Domain Name System-Server (DNS-Server). Wenn nun ein Anwender einen Server noe.wifi.at anwählt, so "fragt" die Station zunächst beim DNS-Server des Anwenders (der meist beim Provider steht), ob er die IP-Adresse von noe.wifi.at kennt. Das wird nicht der Fall sein. In diesem Fall hat der DNS-Server die IP-Adresse des nächstliegenden DNS-Servers gespeichert und fragt bei diesem an, ob er die IP-Adresse kennt. Das geht so lang, bis ein DNS-Server erfolgreich ist, die IP-Adresse wird übermittelt, die Datenübertragung kann beginnen.

Das Internet ist also ein so genanntes **Teilstrecken-Netzwerk**; es genügt, wenn jeder Internet-Knotenrechner mit einem weiteren Knoten verbunden ist. Die physikalische Datenübertragung wird über äußerst leistungsfähige Kabel, so genannte "Backbones" realisiert.

Eine Karte, die die europäische Struktur der Backbones zeigt, findet man unter www.ebone.net/structure/backbone.html

Die zentrale Verwaltung der Domain-Namen mit den Top-Level-Domains .com, .net, .org und .int obliegt der **InterNIC**, einer Kooperation aus dem kommerziellen Unternehmen **NSI** (*Network Solutions Inc.*), der Telefongesellschaft AT&T sowie der *US National Science Foundation*. Bisher wurden die angegebenen Domains ausschließlich von der NSI im Auftrag der InterNIC verwaltet. Die jährliche "Miete" eines Domännamens kostet ca. 50 US-$. Die Domain-Verwaltung soll jedoch bis 2001 von der NSI an die nichtkommerzielle Organisation ICANN (International Corporation for Assigned Names and Numbers) übergeben werden. Die Datenbank der NSI ist unter www.networksolutions.com/cgi-bin/whois/whois zu finden.

Die **IANA** (*Internet Assigned Numbers Authority*, www.iana.org) verwaltet die IP-Adressen.

Einen **IP-Adressen-Index** findet man unter ipindex.dragonstar.net.

Die **ISPA** (*Internet Service Provider Association Austria* - www.ispa.at) ist die Vereinigung der österreichischen Internet Service Provider, quasi eine "Dachorganisation". Die **NIC.AT** GmbH, ein Unternehmen der ISPA, ist mit der Verwaltung und Vergabe der Domänennamen mit dem Top Level Domain ".at" beauftragt (www.nic.at). Registrierungen und Online-Abfragen von at-Domainen sind unter www.namen.at möglich.

Dabei gibt es zum Beispiel als Länder-Top Level Domain (ISO-Norm 3166):

`at`	Austria (Österreich)
`de`	Deutschland
`jp`	Japan
`us`	USA (fehlt meist)

Zusätzlich zu den landesspezifischen Erweiterungen gab es folgende Kennzeichnungen, die ursprünglich nur US-amerikanischen Einrichtungen vorbehalten waren:

`com`	company (Firma)
`gov`	government (Regierung) - US
`edu`	education (Universitäten) - US
`mil`	military (Militär) - US
`int`	internationale Organisation
`org`	organization (gemeinnützige Organisation)
`net`	Provider

Nun werden die Adressen von 28 lizenzierten Firmen vergeben. Diese Firmen werden im **CORE** (*Council of Registrars*) zusammengefasst. Die neuen TLDs lauten:

`firm`	Firmen und Unternehmen
`arts`	Kunst und Kultur
`info`	Informationsservices
`rec`	Unterhaltung und Freizeit
`web`	WWW-Aktivitäten
`store`	Warenangebote
`nom`	Restkategorie

3 Erstellen einer einfachen Homepage

Alle Seiten im WWW sind in einer einheitlichen "Sprache" erstellt worden: **HTML** = *HyperText Markup Language*.

Obwohl es heute bereits Programme gibt, mit denen HTML-Seiten einfach so wie "normale" Word-Dokumente erstellen werden können, ist es von Vorteil, einige Grundbegriffe der HTML (HyperText Markup Language) zu verstehen.

HTML-Dokumente bestehen aus reinem ASCII-Text, der spezielle **HTML-"Befehle"** (*Tags*) enthält. HTML-Dokumente können also mit jedem Editor erstellt werden (also etwa `edit` in DOS oder `vi` oder Emacs in UNIX)! Es gibt allerdings bereits eine Unzahl an Programmen, die den Anwender bei der Entwicklung von WWW-Seiten unterstützen, indem sie WYSIWYG-fähig sind. So ist es möglich, mit Programmen der Microsoft-Bürosuite Office 2000 erstellte Dokumente (Word, Excel, Powerpoint usw) als HTML-Datei abzuspeichern.

So gesehen, kann man mehrere Arten von Programmen unterscheiden, die es dem Anwender ermöglichen, eine Homepage zu erstellen:

1. Editoren (für den Programmier-Freak): Hier kann man nur reinen Text eingeben; spezielle Internet-Editoren helfen dem Programmierer allerdings durch Anzeigen von Vorschau-Bildern.

Dazu zählt:

- der Windows-Editor NOTEPAD.EXE
- Allaire Homesite (bereits mit speziellen Internet-Funktionen)

2. Gestaltungswerkzeuge für den Privatbereich (wenig professionell)

Hier unterscheidet man Programme unterschiedlicher Professionalität:

- Microsoft FrontPage Express: gratis (beim Internet Explorer dabei), wenig Funktionen
- Microsoft Word 2000: zur Not verwendbar (mit dem Menüpunkt [Datei]-[Als Webseite speichern]
- Microsoft FrontPage 2000: bei Webdesignern unbeliebt (Seiten funktionieren oft nicht, sind schwer änderbar); gut geeignet für kleine private Seiten, bei denen ein schneller Erfolg wesentlich ist
- NetScape Composer: gratis, entspricht FrontPad
- Adobe PageMill: das Web-Produkt für das Heimbüro von Adobe, wesentlich bessere Möglichkeiten als bei FrontPage
- Corel WebMasterSuite

3. Gestaltungswerkzeuge für den professionellen Webdesigner

Nur wenige Produkte teilen sich den professionellen Webdesign-Markt; sie sind umfangreich, aber meist teuer:

- HotMetal Pro (SoftQuad)
- Adobe GoLive
- Macromedia Dreamweaver (aktuelle Version 3)
- NetObjects Fusion

Für den Beginn seien auch folgende WWW-Links empfohlen:

- www.boku.ac.at/htmleinf
- www.eu.microsoft.com/frontpage
- ourworld.compuserve.com/homepages/muenz/selfhtml.zip
- www.sgdev.com
- www.ideenreich.com/drweb.shtml

Vor allem der Lehrgang von Stefan Münz ist wirklich ausführlich und gelungen - sehr zu empfehlen!

XML (*Extensible Markup Language*) wird das Dateiformat HTML mittelfristig ablösen. Unterschied zu HTML ist etwa, dass im Code eigene Tags ("Befehle") definiert werden können, die alle bisherigen Browser-spezifischen Erweiterungen unnötig machen.

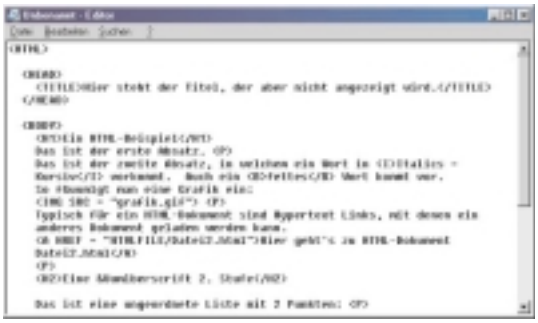
CSS (*Cascading Style Sheets*) erleichtern das Erstellen von Slidebars und Navigationsschaltflächen.

Wir verwenden den Windows-Editor NOTEPAD.EXE!

Wichtig: Stellen Sie zunächst im Arbeitsplatz die Ordneroptionen um (***[Extras] - [Ordneroptionen]***):

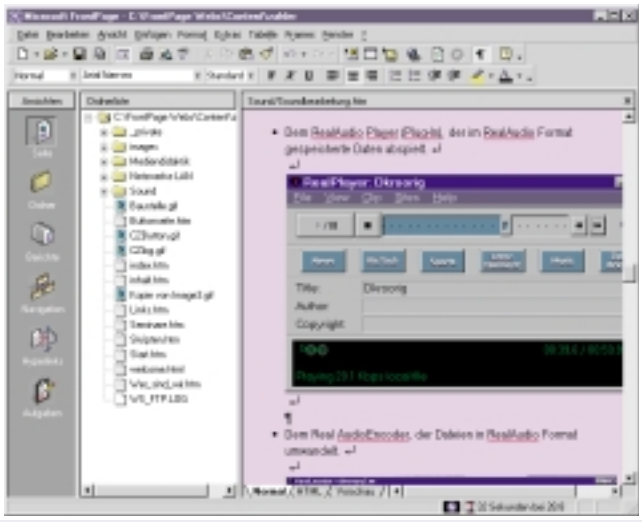
Starten Sie den Windows-Editor (***Start - Programme - Zubehör - Editor***); geben Sie untenstehenden HTML-Code ein:

```
<HTML>
  <HEAD>
    <TITLE>Hier steht der Titel.</TITLE>
  </HEAD>
  <BODY>
    <H1>Ein HTML-Beispiel</H1>
    Das ist der erste Absatz. <P>
    Das ist der zweite Absatz, in welchem ein Wort in <I>Italics =
    Kursiv</I> vorkommt.  Auch ein <B>fettes</B> Wort kommt vor.
    So f&uumlgt man eine Grafik ein:
    <IMG SRC = "grafik.gif"> <P>
    Typisch für ein HTML-Dokument sind Hypertext Links, mit denen ein
    anderes Dokument geladen werden kann.
    <A HREF = "HTMLFILE/Datei2.html">Hier geht's zu HTML-Dokument
    Datei2.html</A>
    <P>
    <H2>Eine &Uuml;berschrift 2. Stufe</H2>

    Das ist eine ungeordnete Liste mit 2 Punkten: <P>
    <UL>
      <LI> Punkt 1
      <LI> Punkt 2
    </UL>

    <P>
    Wenn noch Fragen sind, senden Sie eine Email an:
    <A HREF = "mailto: office@zahler.at"> Christian Zahler </A>
    Hier ist das Beispiel zu Ende. <P>
  </BODY>
</HTML>
```

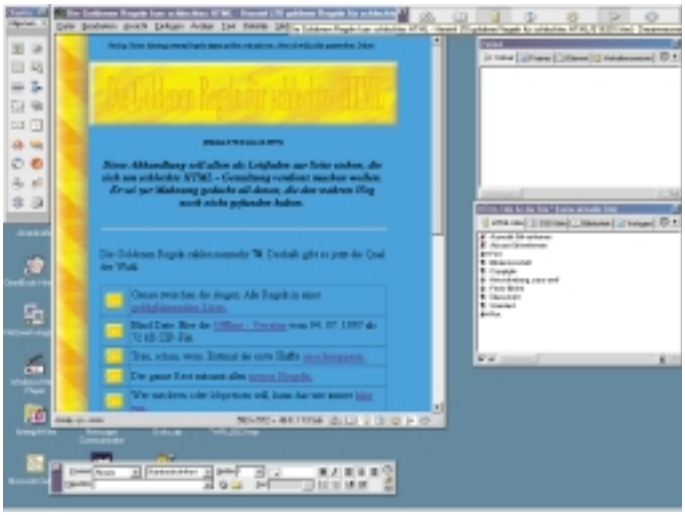


Speichern Sie das HTML-Dokument nun (Vorschlag: **HOMEPAGE.HTM**):

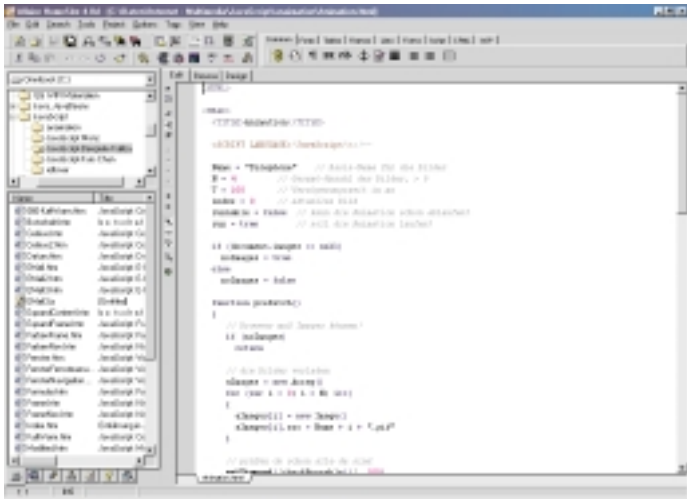
Sie finden Ihre Homepage bereits mit



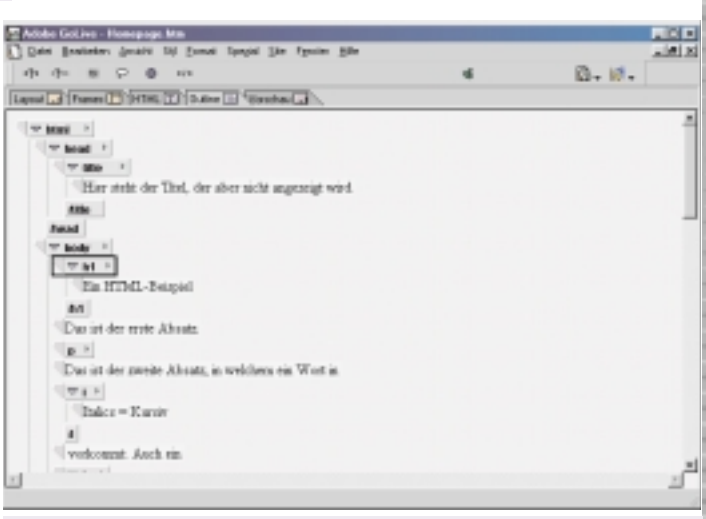
Screenshot: Microsoft Frontpage 2000



Screenshot: Macromedia DreamWeaver 3

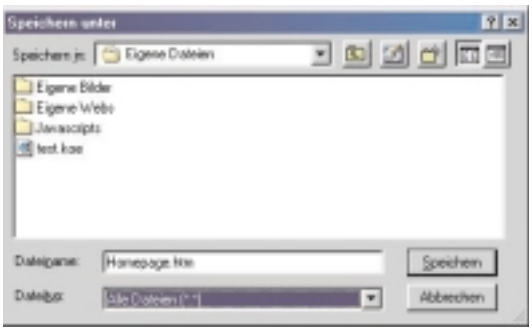


Screenshot: Allaire Homesite 4.0

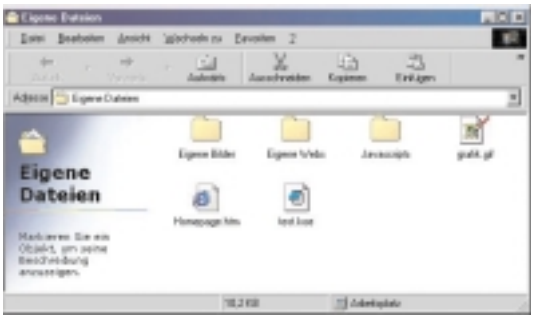


Screenshot: Outline-Ansicht in Adobe GoLive 4.0

dem typischen Dateisymbol versehen:



Wenn Sie auf das Dateisymbol doppelklicken, sehen Sie die Homepage so, wie sie der Benutzer sehen würde, der im Internet surft:



Im Browser erscheint der Text formatiert, hier in der Editoransicht findet man den Text zwischen Zeichenfolgen, die in spitzen Klammern eingeschlossen sind. Das sind Tags (*tag* engl. Schildchen, Etikett, *to tag* markieren), die Beschreibung der Formatierung.

Liste der wichtigsten Formatbefehle (Tags)

Die Tags klammern paarweise gewisse Bereiche ("*Container Tags*"):

`<HTML>`	`</HTML>`	der gesamte Text.
`<HEAD>`	`</HEAD>`	der Kopf
`<TITLE>`	`</TITLE>`	im Kopf des Doku-mentes steht der Titel, der im Browser in der Titelleiste erscheint
`<BODY>`	`</BODY>`	klammert alles übrige
`<H1>`	`</H1>`	die größte Überschrift
`<H2>`	`</H2>`	bis
`<H6>`	`</H6>`	jeweils kleinere Überschriften.
`<P>`	`</P>`	ein Absatz, ein Paragraph.
`<UL>`	`</UL>`	eine Liste mit Aufzählungspunkten (Unordered List).
`<OL>`	`</OL>`	eine Liste mit Numerierung (Ordered List).
`<LI>`	`</LI>`	innerhalb der Listen die einzelnen Zeilen.

Tags kommen auch einzeln vor (Leere Formatbefehle):

` `	ein Zeilenumbruch (BReak).
`<HR>`	eine horizontale Linie (Horizontal Ruler)

Umlaute und ß sind eine Eigenheit der deutschen Sprache. Damit sie richtig übertragen werden, sollten sie nicht direkt eingegeben werden, sondern "maskiert" werden, das bedeutet, sie sollten mit Zeichenkürzeln umschrieben werden. Das macht den Text im Editor schwer lesbar. Zeichenkürzel fangen mit & an und hören mit einem Strichpunkt auf.

`&auml;`	ä (a-Umlaut)
`&Auml;`	Ä (A-Umlaut)
`&ouml;`	ö (o-Umlaut)
`&Ouml;`	Ö (O-Umlaut)
`&uuml;`	ü (u-Umlaut)
`&Uuml;`	Ü (U-Umlaut)
`&szlig;`	ß (sz-Ligatur, scharfes s)
`&copy;`	© (Copyright)
`&amp;`	& (Ampersand)
`&quot;`	doppeltes Anführungszeichen oben (quotation mark)
`&lt;`	< (less than)
`&gt;`	> (greater than)
` `	unbedingtes Leerzeichen (**n**on-**b**reaking **spa**ce)

Erhöhung der Zahl der für Suchmaschinen relevanten Begriffe:

```
<META name="description" content="Beschreibung der Webseite">
<META name="keywords" content="Stichwörter zu Ihrem Angebot">
```

Links

Ein Link ist eine farbig hervorgehobene und unterstrichene Stelle oder ein Bild im Text des Browsers. In der Umgebung des Links verwandelt sich im Browser der Mauszeiger in eine Hand. Wenn man mit der linken Maustaste darauf klickt, dann springt man zu einer anderen Textstelle im eigenen Text, zu einem Dokument auf demselben Computer oder zu irgendeinem Dokument auf einem Server in der Welt.

In der Editoransicht im Bild oben steht:

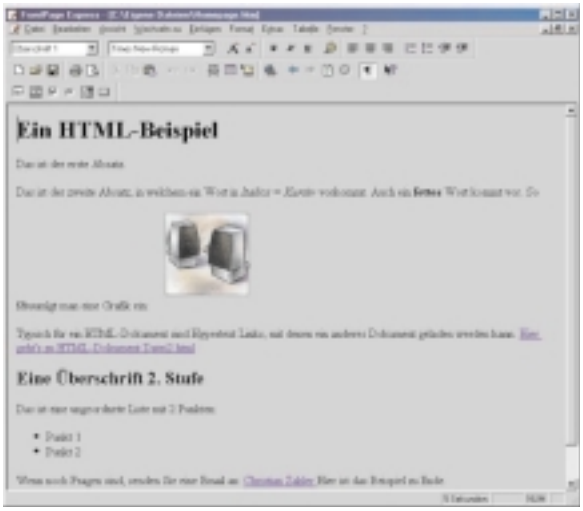
```
<A HREF="Seite2.htm">.....</A>
```

Allgemein `<A HREF=` URL `>.....</A>`

Ein **URL**, ein *Uniform Resource Locator* ist die Sprungadresse, zu der man springt, wenn man den "Anker" anklickt. Im Text steht hier dafür das Wort Links. Man springt von hier zu einem Dokument mit dem Namen `Seite2.htm`.

`<A HREF...>` steht für *Anchor Hypertext Reference*.

Wir versuchen es mit FrontPage Express!



Mit diesem einfachen WYSiWYG-Editor (*what you see is what you get* - am Bildschirm schaut die Seite genauso aus wie im Internet) ist es möglich, die Seitenerstellung fast so zu machen wie mit Word.

Entsprechende Kurse finden Sie im Kursbuch des Wifi Niederösterreich und im Internet unter *http://www.noe.wifi.at/*

4 FTP (So holen Sie sich Treiber und Spiele und bringen Ihre Homepage ins Internet!)

Mit **FTP** (*File Transfer Protocol*, also Dateiübertragungsprotokoll) können Sie Dateien von Ihrem Rechner auf einen entfernten Server übertragen (*Upload*) oder von einem entfernten Server Dateien auf Ihren Rechner laden (*Download*).

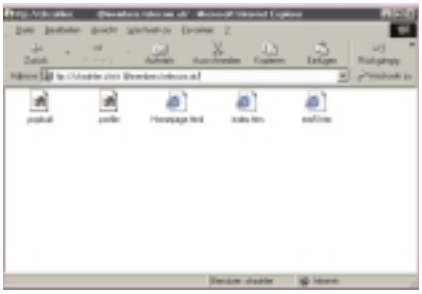
Der FTP-Dienst ist auf verschiedene Art und Weise nutzbar:

FTP über den Browser:

Auch über Browser-Software ist eingeschränkter FTP-Betrieb möglich: Während Downloads problemlos möglich sind, können Uploads nicht durchgeführt werden!

Man kann Programme, Treiber, Spiele, Dokumente - also alles Mögliche - auf seinen Rechner "herunterladen" also "downloaden".

Dazu gibt man im Browser die Adresse ein. Das Protokoll heißt "ftp". Daher ist statt **`http:// ftp://`** einzugeben (kann man aber auch automatisch ergänzen lassen).



Anmerkung: Das Passwort in der obigen Abbildung wurde abgedeckt bzw. verändert.

Beispiele für FTP-Server:

`ftp://ftp.vip.at/`

Und dann verfolgen Sie die Verzeichnisse - wie im Windows-Explorer

Für einen FTP-Zugriff ist notwendig (ein Browser managed das selber):

Eine Benutzerkennung (User-ID). Viele Server erlauben anonymen Zugang mit der benutzerkennung **`anonymous`**.

- Ein Passwort (bei Anonymzugriff Eingabe der E-Mail-Adresse) .

Wenn Sie statt Ordnern Dateien (*Files*) sehen, dann können Sie die gewünschte auswählen und der Download beginnt. Während des Downloads können Sie in verschiedenen Browser-Fenstern weitersurfen.

Wichtig: Sollten Sie für den FTP-Server einen Benutzernamen und ein Kennwort eingeben müssen, dann wählen Sie bitte folgende Syntax für die Adresszeile des Browsers:

`ftp://Benutzername:Kennwort@ftpserver.at`

()

Tipps

- Wenn Sie anonym eingestiegen sind, dann verfolgen Sie die Gasse im Verzeichnis "pub" (steht für "public", also "öffentlich")
- Wegen Virusgefahr holen Sie Programme nur von vertrauenswürdigen Sites (*Site*, engl. Niederlassung, gemeint ist die des Servers)

Der Download ist unkritisch, aber bei der Installation könnte es passieren ...

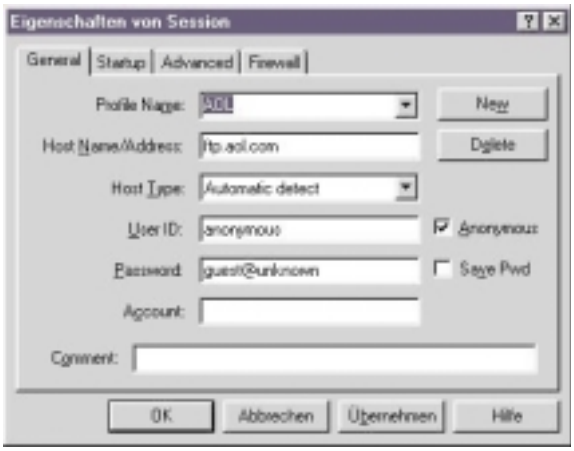
- Schützen Sie sich durch ein Antiviren-Programm, Sichern Sie Ihre Daten.
- Downloads gehen außerhalb der "Rush-Hours" schneller
- Wählen Sie "nahe" Server
- Speichern Sie Downloads in einem eigenen, von Ihnen angelegten Verzeichnis

Wenn Sie Programme installieren, verschieben (oder kopieren) Sie die Datei in ein leeres Verzeichnis, sonst haben Sie u.U. alles unübersichtlich in einem Verzeichnis und wissen nicht mehr, was wohin gehört!

Spezielles FTP-Programm

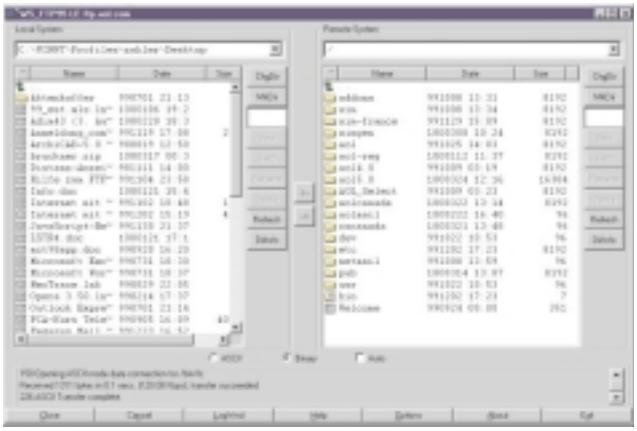
zum Beispiel WS-FTP

1. Starten Sie das Programm WS-FTP95
2. Legen Sie ein Profil mit folgenden Einträgen an (Klicken Sie auf die Schaltfläche "New"):



Mit "OK" verbinden Sie sich zum America-Online-FTP-Server: Links sehen Sie die Verzeichnis-/Laufwerksstruktur Ihres eigenen Rechners, rechts sehen Sie die Verzeichnisstruktur des FTP-Servers, mit dem Sie verbunden sind.

4. Mit den Pfeilen in der Mitte können Sie markierte Dateien von Ihr



er Festplatte (links) auf den Server (rechts) kopieren oder umgekehrt!

Manuelle FTP-Sitzung:

Aufruf:

ftp Servername

FTP-Befehle:

`!`	**`delete`**	**`literal`**	**`prompt`**	**`send`**
`?`	**`debug`**	**`ls`**	**`put`**	**`status`**
`append`	**`dir`**	**`mdelete`**	**`pwd`**	**`trace`**
`ascii`	**`disconnect`**	**`mdir`**	**`quit`**	**`type`**
`bell`	**`get`**	**`mget`**	**`quote`**	**`user`**
`binary`	**`glob`**	**`mkdir`**	**`recv`**	**`verbose`**
`bye`	**`hash`**	**`mls`**	**`remotehelp`**	
`cd`	**`help`**	**`mput`**	**`rename`**	
`close`	**`lcd`**	**`open`**	**`rmdir`**	

`dir`	remote Verzeichnis auflisten
`cd, lcd`	Verzeichnis wechseln, remote / local
`pwd`	aktuelles Verzeichnis
`get, mget`	Datei/en von remote nach local kopieren
`put, mput`	Datei/en von local nach remote kopieren
`binary`	auf binären Transfer (Programme, Images, ...) umschalten
`prompt`	Bestätigung abschalten
`user`	als Benutzer einloggen
`open, close`	Verbindung öffnen / schließen
`?`	Hilfe anzeigen
`quit, bye`	Programm beenden

Beispiel für eine manuelle FTP-Sitzung (Benutzereingaben sind fett dargestellt):

```
C:\WIN98>ftp off97.noe.wifi.at
Verbindung mit off97.noe.wifi.at.
220 wifi2 Microsoft FTP Service (Version 3.0).
Benutzer (off97.noe.wifi.at:(none)): user401
331 Password required for user401.
Kennwort:****
230-Herzlich Willkommen am Wifi Ftp-Server !
230 User user401 logged in.
Ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
d---------   1 owner    group       0 Aug 19  1999 kids
d---------   1 owner    group       0 Feb 17  1998 kktn
----------   1 owner    group       0 Aug 18  1999 test.txt
----------   1 owner    group       0 Aug 19  1999 test3.txt
226 Transfer complete.
Ftp: 269 Bytes empfangen in 0.16Sekunden 1.68KB/Sek.
Ftp> get test.txt
200 PORT command successful.
150 Opening ASCII mode data connection for test.txt(0 bytes).
226 Transfer complete.
Ftp> put xxx.htm
200 PORT command successful.
150 Opening ASCII mode data connection for xxx.htm.
226 Transfer complete.
Ftp: 1777 Bytes gesendet in 0.00Sekunden 1777000.00KB/Sek.
Ftp> pwd
257 "/" is current directory.
Ftp> quit
221 Auf Wiedersehen !
```

Wenn Sie als anonymer FTP-Nutzer arbeiten wollen, so geben Sie als Benutzername **anonymous** an, als Kennwort **Ihre eigene E-Mail-Adresse**. (Es ist kein Passwort nötig, allerdings verlangen die Regeln der Netiquette eine derartige - freiwillige! - Identifizierung.)

Archie: Die ftp-Suchmaschine

Mit "Archie" können Sie nach Dateien, Treibern, u.s.w. suchen. Sie wissen den Dateinamen, aber Sie kennen keinen ftp-Server? Über einen Archie-Server lässt sich dieses Problem lösen.

Die Suche erfolgt praktisch wie mit einer normalen Suchmaschine, nur geben Sie nun einen Dateinamen an. Die Suchergebnis-Seiten zeigen wieder Links zu den Servern und den Dateien.

Links / Tipps / Tricks

- *http://archie.rutgers.edu/* (stehen meist in Universitäten)
- Exact match: bedeutet: Dateiname wurde genau eingegeben und es soll auch nur dies gesucht werden
- Substring bedeutet: Dateien die "so" anfangen werden gesucht
- Suchen Sie nach anderen Archie-Servern in "normalen" Suchmaschinen mit dem Begriffen "archie server". Versuchen Sie auch diese.
- Wenn Sie Software per Beschreibung - also nicht per Dateinamen - suchen wollen, dann bedienen Sie sich einer "normalen" Suchmaschine bzw. einer auf "Software" spezialisierten Suchmaschine z.B.: *http://www.download.com/*

5 Komprimieren von Dateien mit WinZip

Wenn Sie Mail-Attachments (Dateianhänge) mit E-Mails verschicken, sollten Sie auf geringe Dateigrößen achten! Es hat sich eingebürgert, keine Dateien ungefragt abzusenden, die größer als 300 KB sind.

Seien Sie fair - der E-Mail-Empfänger hat unter Umständen eine schlechte Verbindung und benötigt Stunden, um Ihr E-Mail herunterzuladen!

Eines der verbreitetesten Programme zum Komprimieren (Verkleinern) von Dateien ist das Programm **WinZip**.

Das Programm WinZip können Sie auf der Seite *www.winzip.com* herunterladen! Die "Evaluation Version" ist voll funktionsfähig; jedoch erhalten Sie bei jedem Aufruf eine Werbung mit der Aufforderung, das Programm registrieren zu lassen.

Zum Zeitpunkt der Erstellung dieses Skriptums war die aktuelle **Version 7** erhältlich, **Version 8** erst als Beta-Version verfügbar.

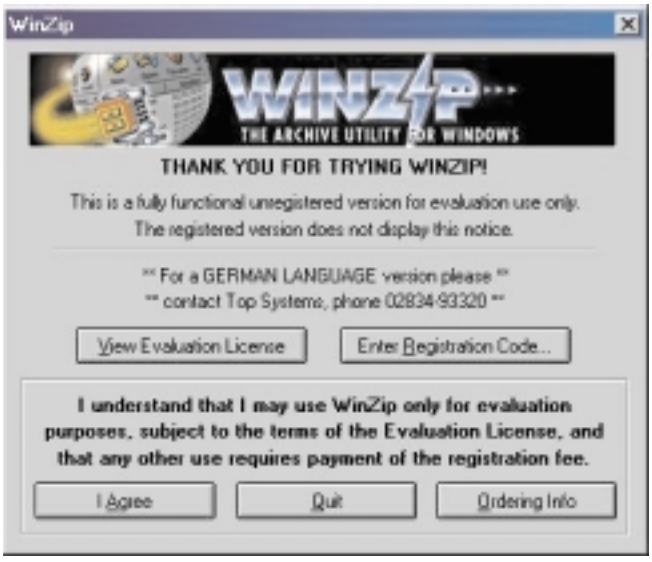
Vorteile des "Zippens"

- Komprimierte Dateien sind (meist) kleiner (bereits komprimierte Bilder .gif und .jpg lassen sich nicht weiter komprimieren)
- Man kann in eine Zip-Datei mehrere Dateien hineinverpacken
- Ein Zip-Archiv kann als Container für viele Dateien dienen. Beim öfteren Weitergeben kann nichts verloren gehen.
- In eine Zip-Datei lassen sich ganze Verzeichnis-Bäume hineinverpacken (Subfolder anklicken). Diese Bäume werden beim Entpacken (unzip) auch am Zielrechner wieder eingerichtet!
- Alle Installationsdateien (Software) sind nach diesem Verfahren verpackt.

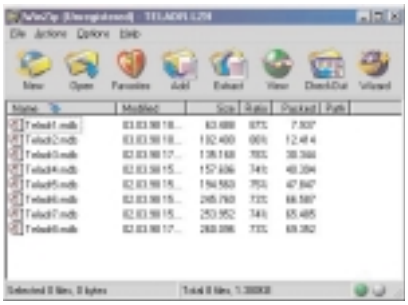
Komprimieren einzelner Dateien

Klicken Sie mit der rechten Maustaste auf die zu komprimierende Datei. Ist das Programm WinZip installiert, so finden Sie im Kontextmenü zwei WinZip-Einträge: Mit [*Add to Zip*]

wird das Programm WinZip aufgerufen, Sie müssen dann einen Dateinamen für die komprimierte Datei eingeben sowie festlegen, in welchem Ordner die komprimierte Datei gespeichert werden soll. Der zweite Eintrag *[Add to Dateiname.zip]* arbeitet vollautomatisch - die komprimierte Datei wird unter demselben Dateinamen wie die ursprüngliche Datei im selben Ordner abgelegt.



Wenn Sie die Evaluation Version verwenden, müssen Sie bei jeder Aktion die Schaltfläche *"I Agree"* betätigen (damit erklären Sie sich mit den Lizenzbedingungen einverstanden).



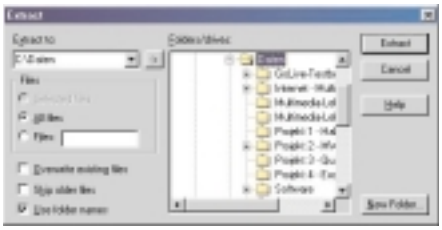
Komprimieren mehrerer Dateien

1. Starten Sie Winzip
2. Öffnen Sie den Windows-Explorer und markieren Sie Dateien
3. Ziehen Sie markierte Dateien in den weißen Bereich des Winzip-Fensters
4. Vergeben Sie einen "Archiv-Namen" und "OK"
5. Sie haben jetzt eine .zip-Datei, die Sie versenden kännen.

Dekomprimieren von Dateien

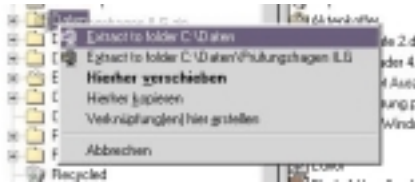
Wenn Sie auf eine komprimierte Datei doppelklicken, wird ihr Inhalt angezeigt:

Mit "Extract" können Sie die komprimierten Dateien in einen Ordner Ihrer Wahl extrahieren:



Verschieben/Kopieren mit gleichzeitigem Dekomprimieren von Dateien:

Es ist auch möglich, während eines Kopier- oder Verschiebevorgangs (Ziehen mit der rechten Maustaste) eine Dekomprimierung durchzuführen:



Welche Archivformate werden von WinZip 7.0 unterstützt?

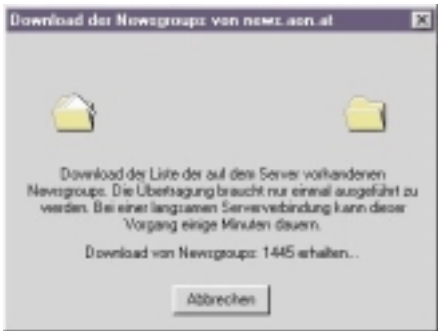
- ***.ZIP**: Am häufigsten verwendet, kann auf mehrere Disketten verteilt werden, Kompression wird unterstützt, mehrere Dateien können in ein Zip-Archiv komprimiert werden.
- ***.TAR, *.Z, *.TAZ, *.TGZ**: oft auf Unix-basierten Internet-Seiten zu finden. TAR bedeutet "Tape ARchive". Es kann nicht komprimieren, nur gruppieren. Winzip kann diese Dateien öffnen und dekomprimieren, aber keine derartigen Dateien anlegen.
- **UUencoded, XXencoded, BinHex, MIME**: häufig für Internet E-Mail verwendet. WinZip kann solche Dateien öffnen und extrahieren.
- **Microsoft COMPRESS.EXE**-Format: Solche Dateien sind meist am Underscore am Ende der Dateierweiterung erkennbar, zum Beispiel "commdlg.dl_". Wurde in Microsoft Windows 3.1 und DOS verwendet. Solche Dateien sind mit WinZip 7.0 extrahierbar.
- ***.CAB**: Microsoft Cabinet-Dateien werden zur Installation von Windows 95, 98, 2000 und NT verwendet. WinZip kann solche Dateien öffnen und extrahieren.
- **ARC, ARJ, LZH**: Hier benötigen Sie eine Zusatzsoftware, damit WinZip diese Formate lesen kann! (Etwa ARJ.EXE usw.)

Tipps

- .zip-Dateien an Empfänger versenden, die mit dieser Technik nicht vertraut sind, ist nicht anzuraten, da diese Dateien nur mit einem installierten Winzip-Programm wiederhergestellt werden können.
- Machen Sie folgendes: Nachdem Sie eine .zip-Datei erstellt haben, wandeln Sie diese in eine .exe-Datei um. Sie können das unter *[Actions]-[Make EXE-File]* tun. Diese .exe-Datei ist dann selbstextrahierend und der Empfänger kann sie ganz einfach durch Doppelklick expanieren.

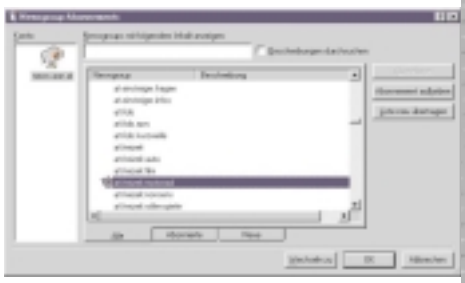
6 Diskussionsgruppen (Newsgroups) als Problemlöser

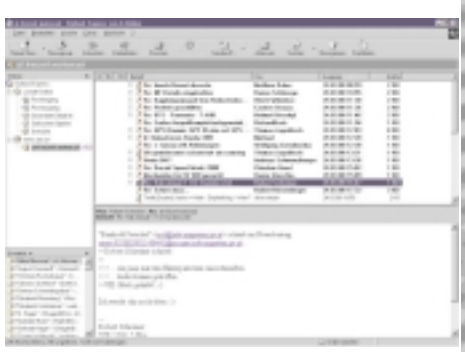
Die *Usenet Newsgroups* sind Diskussionsgruppen, man könnte sie auch als "Selbsthilfegruppen" bezeichnen. Diese sind nicht mit den Chat-Rooms zu vergleichen. Newsgroups - auch kurz "News" genannt - funktionieren auf Basis von E-Mails. Zugriff auf die Newsgoups hat man z.B. in Outlook-Express (OE) unter *[Extras]-[Newsgroups]*.



Wenn man das erste Mal im OE in die Newsgroups einsteigt, wird eine lange Liste der Newsgroup-Namen geladen, dies kann einige Minuten in Anspruch nehmen. Es gibt nämlich im Internet ca. 50.000 Diskussionsgruppen. In vielen dieser Diskussionsgruppen sind tausende Diskussionsbeiträge gespeichert

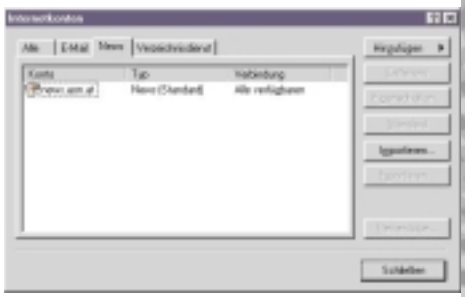
Wenn man in einer Diskussionsgruppe mitdiskutieren möchte, dann sollte man sie "**abonnieren**". Dies ist mit keinen Kosten verbunden, wie man vielleicht meinen könnte. Durch das Abonnieren bekommt man beim nächsten Einstieg nur mehr die Beiträge geliefert, die man noch nicht gelesen hat, bzw. die seit dem ersten Einstieg neu eingelangt sind. Die Korrespondenz erfolgt wie beim E-Mailing. Das Abonnement kann jederzeit wieder aufgehoben werden (auch mit rechter Maustaste auf den Newsgroup-Ordner: "Abonnement aufheben").





Tipps

- Falls noch nicht geschehen, müssen Sie einen News-Server unter [Extras]-[Konten], Karteikarte [News] Den Ihres Providers oder z.B. news.via.at



- Halten Sie sich an die Netiquette:
  - NICHT BRÜLLEN (=keine Großschreibung wie im Beispiel)
  - Lesen Sie erst die vorhandenen Beiträge
- o Fragen Sie nichts, was schon behandelt und beantwortet wurde!
- o Seien Sie höflich, Sie haben es mit Menschen zu tun!
- Namen der Newsgroups z.B.: `rec.photo.digital` `rec`=recreation / Erholung, `alt`= alternative Themen und so weiter. Diese Klassifizierung ist nicht (mehr) wirklich ernst zu nehmen

Probleme lösen mit Newsgroups

Sie haben ein Problem?

Sie brauchen Unterstützung für eine Software, Sie haben ein Installationsproblem? Sie haben ein gesundheitliches Problem? Sie wollen sich eine digitale Foto- oder Video-Kamera kaufen oder ein neues Auto?

Sie glauben, Sie sind mit Ihrem Problem alleine auf der Welt?

Sicher nicht. Ihr Problem haben schon Hunderte vor Ihnen gehabt! Vielleicht haben aber die schon eine Lösung gefunden, oder haben sich gegenseitig (in den Newsgroups) beraten?

Mag schon sein, aber wie finden Sie diese Beiträge?

Suchmaschine für Diskussionsbeiträge

Es gibt im Internet auch die Möglichkeit, nach Diskussionsbeiträgen zu suchen. Viele Suchmaschinen bieten diese Möglichkeiten (Newsgroups, Usenet). Der Klassiker unter diesen Spezialisten ist DEJA (früher Deja-News) http://www.deja.com/. Die Benutzung erfolgt nach den Regeln, die schon bei den "normalen" Suchmaschinen besprochen wurden.

Suchen Sie in http://www.deja.com/ nach der Seite für die Eingabe der Suchworte. Geben Sie die Suchbegriffe in das Formular ein und drücken Sie "Enter". Sie erhalten eine Linkliste zu den gefundenen Beiträgen.

Deja sucht quer über alle Newsgroups.

Da in den Newsgroups auch über Produkte und Modelle diskutiert wird, wird hier "Klartext" gesprochen. Hier erfahren Sie, was "gut" und was "schlecht" ist. Bevor Sie sich für ein Produkt entschließen, schauen Sie in die Newsgroups.

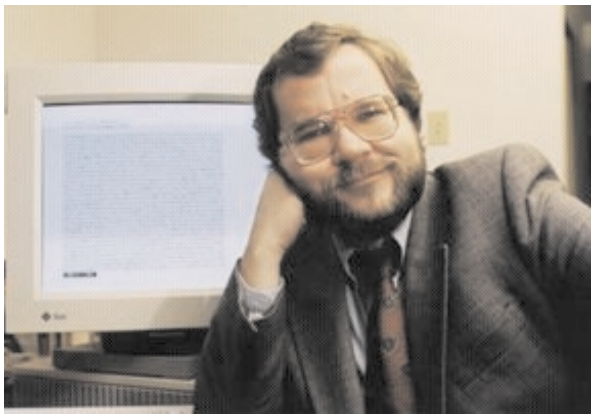
Tipps

- Verfolgen Sie einen Diskussionsfaden ("Thread" in deja). Im Outlook Express sehen Sie ein "+" vor dem Einstiegsbeitrag.
- Suchen Sie mit Suchmaschinen wie "deja", diskutieren Sie in Outlook Express! Sie können via deja auch Beiträge abschicken, aber die Verfolgung einer Diskussion ist dann eher mühsam.
- Senden Sie in Outlook Express Antworten auf Beiträge mit "Newsgroup antworten", damit andere Ihren Beitrag lesen können. Nur in Einzelfällen antworten Sie direkt an die E-Mail-Adresse des Autors.

7 Verschlüsseln von Daten mit PGP (Pretty Good Privacy)

Wozu?

Im Internet werden die Texte von E-Mails sowie die Eingaben in Formularen im Klartext via mehrere Server zum Empfänger weitergeleitet. "Sniffer-Programme" könnten solche Nachrichten "mitlesen". Es ist daher nicht zu empfehlen, Firmengeheimnisse, Patente, Konstruktionszeichnungen u.s.w. unverschlüsselt zu versenden. Sie brauchen aber nicht auf die elektronische Übertragung zu verzichten, entsprechende Verschlüsselungsprogramme sind im Internet verfügbar.



Phil Zimmermann (Quelle: www.pgp.com)

Dies führte zur Entwicklung von Verschlüsselungstechniken = **Kryptographie**.

Man unterscheidet:

- **Symmetrische Algorithmen**: Es gibt nur einen Schlüssel (single-key, one-key), der für Ver- und Entschlüsselung verwendet wird. Heute nicht mehr üblich.
- **Asymmetrische Algorithmen**: Es gibt zwei mathematisch verwandte Schlüssel: ein Schlüssel verschlüsselt, der zweite Schlüssel entschlüsselt. Der eine Schlüssel kann aus dem anderen nicht berechnet werden! Diese Algorithmen werden heute sehr häufig verwendet (**Public-/Private-Key-Methode**).

Mathematisch gesehen werden heute zwei Verschlüsselungsmethoden verwendet:

1. RSA-System (Rivest-Shamir-Adleman, 80er Jahre)

Man verwendete üblicherweise 40 Bit Europa-Schlüssel in Europa bzw. 128 Bit-Schlüssel in den USA, Unterschied Faktor 3000.

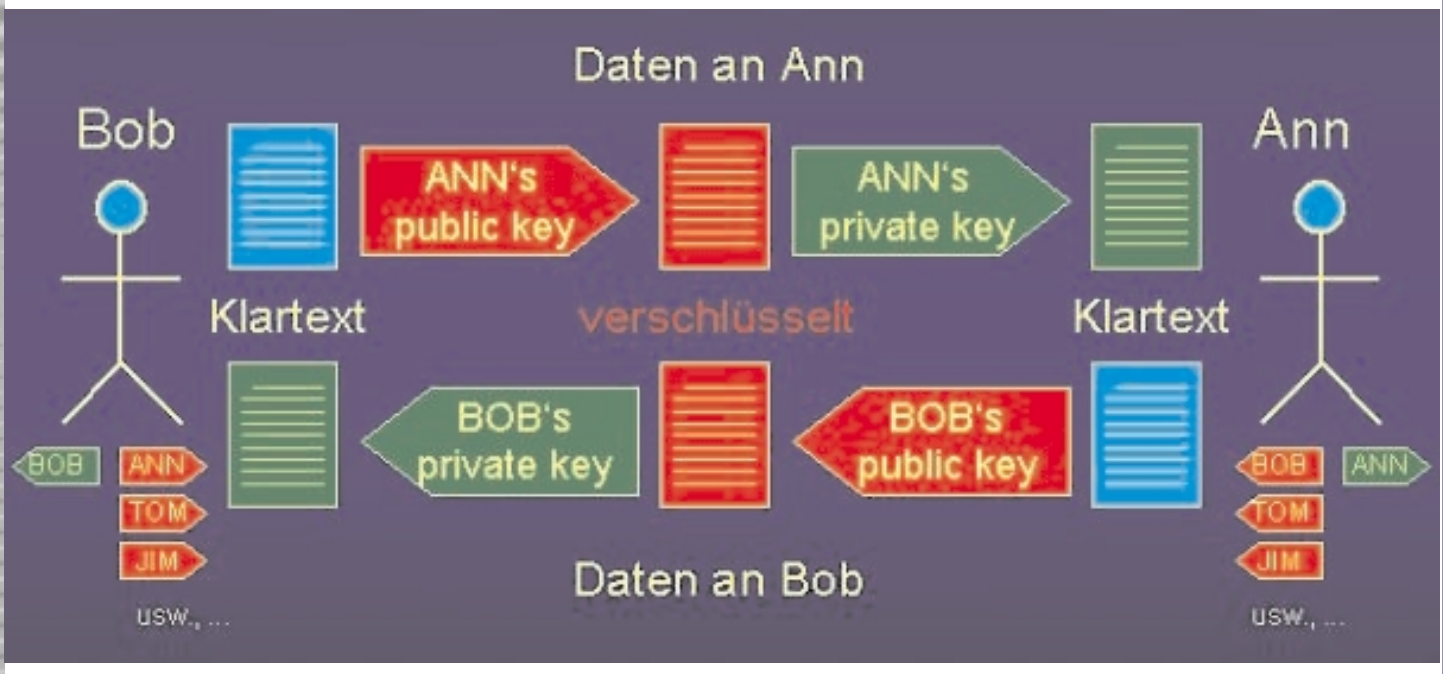
Je mehr Bit ein Schlüssel hat, desto sicherer wird er. Um einen Schlüssel zu "erraten", kann man eine "Brute Force Attack" (Attacke mit brutaler Gewalt) starten; darunter versteht man das simple Ausprobieren aller denkbaren Möglichkeiten (bei einem dreistelligen Code etwa 000, 001, ..., 999).

1984 wurde ein 480 Bit Schlüssel nach 8 Monaten mit 1600 Computern geknackt (5000 MIPS Jahre notwendig); siehe http://rc5stats.distributed.net/.

2. Diffie-Hellman Paare

SInd noch sicherer als das RSA-System, da Schlüssel mit einer Länge von 2048 Bit bzw. 4096 Bit erzeugt werden können.

International durchgesetzt hat sich die Software der Firma PGP (Pretty Good Privacy, "recht gute Privatsphäre"), die



von Philip Zimmermann gegründet wurde.

Diese Software dient zum Verschlüsseln von Dokumenten, E-Mails und Webseiten.

Freeware-Versionen stehen zum Download bereit unter www.pgp.com. Download der internationalen Version von www.pgpi.com. Eine deutsche Version ist auch bereits verfügbar.

Das Verschlüsselungsverfahren gilt derzeit als so sicher, sodass nicht einmal die Geheimdienste in der Lage sind, solche Nachrichten zu entschlüsseln. Deswegen wird auch von den Regierungen vieler Staaten überlegt hier durch Gesetze oder andere Maßnahmen zu gewährleisten, dass der Staat doch noch "mitlesen" kann. In Amerika steht das Verfahren unter dem Kriegswaffengesetz, wonach die amerikanische Version des Programms nicht exportiert werden darf. Die PGP-Software hat sich - trotz Schutzmechanismen seitens der amerikanischen Behörden - in kürzester Zeit weltweit verbreitet.

Wie funktioniert es?

Ann und Bob wollen geheime Nachrichten austauschen. Ann möchte an Bob eine verschlüsselte Nachricht senden. Ann benötigt daher einen Verschlüsselungsschlüssel von Bob. Mit anderen Worten: Wenn Bob verschlüsselte Nachrichten bekommen möchte, dann muss er

1. ein Schlüsselpaar erstellen. Dies wird B in der Regel nur einmal machen.
   Ein Schlüsselpaar besteht aus einem **privaten Schlüssel** ("*Private Key*") und einem **öffentlichen Schlüssel** ("*Public Key*"). Der Private Schlüssel darf nicht hergegeben werden, der Öffentliche Schlüssel kann unbedenklich jedem gegeben werden, ja sogar im Internet auf sogenannten Key-Servern veröffentlicht werden.
2. den öffentlichen Schlüssel an Ann senden.

Ann wird nun:

1. ein E-Mail schreiben,
2. den Text mit dem Öffentlichen Schlüssel von Bob verschlüsseln (dazu braucht sie ein Programm wie z.B. PGP),
3. das verschlüsselte E-Mail versenden.

Bob wird nun:

- 1. das E-Mail öffnen,
- 2. den verschlüsselten Text mit dem Private Key entschlüsseln,
- 3. den entschlüsselten Text lesen.

Erzeugung eines neuen Schlüsselpaares

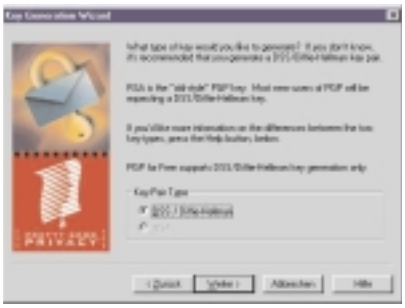
Verschlüsseln, signieren und entschlüsseln in der Praxis

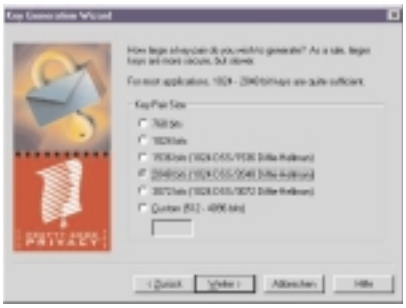
Verschlüsseln von Dateien

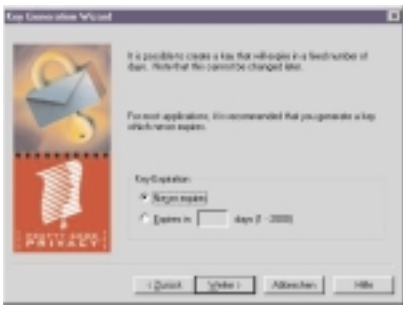
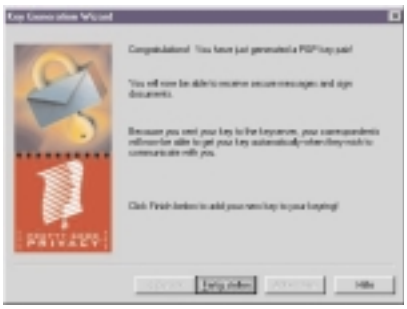
Nach Installation der PGP-Software und Anlegen eines Schlüsselpaares brauchen Sie nur mehr mit der rechten Maustaste auf eine Datei klicken - im Kontextmenü





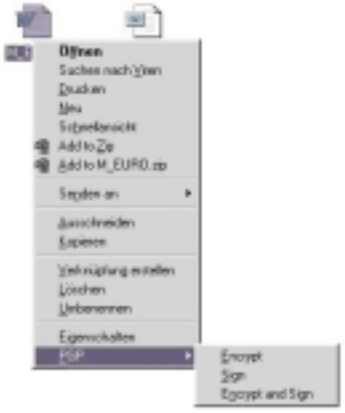




finden Sie den Eintrag "PGP". Mit "En-

crypt" können Sie die Datei verschlüsseln!



PGP zeigt nach der Installation in der Taskleite rechts ein kleines Kuvert mit einem Schloss-Bügel ("Vorhängeschloss"). Dies ist die zentrale Schaltstelle.

Key-Ring = Schlüsselbund

Enthält alle gespeicherten Public-Keys (den eigenen und die der Partner).

Clipboard = Zwischenablage

Über diesen Schlüsselbund kann man mit "New Key" bzw. "Neuer Schlüssel" einen Assistenten starten, der durch die Erstellung eines (eigenen) Schlüsselbundes führt. Folgen Sie den Anweisungen.

E-Mail schreiben und Text verschlüsseln

1. E-Mail schreiben (wie gewohnt)
2. Text Markieren und in die Zwischenablage kopieren (Strg C bzw. Strg X oder ***Bearbeiten: Kopieren*** oder ***Ausschneiden***)
3. PGP-Schaltstelle anklicken (s.o.)
4. "Encrypt Clipboard" oder "Zwischenablage verschlüsseln" auswählen. In der Zwischenablage steht jetzt der verschlüsselte Text
5. Strg V oder ***Bearbeiten: Einfügen*** Der verschlüsselte Text wird aus der Zwischenablage eingefügt.
6. E-Mail wie gewohnt versenden

E-Mail mit verschlüsseltem Text kommt

1. E-Mail wie gewohnt öffnen
2. Verschlüsselten Text markieren. Einschließlich der ersten und der letzten Zeile!
3. Strg C bzw.. ***Bearbeiten:Kopieren***. Text in die Zwischenablage kopieren
4. PGP-Schaltstelle anklicken und
5. "***Decrypt/Verify Clipboard***" oder "***Zwischenablage entschlüsseln***" auswählen.
   Berechtigung wird anhand der einzugebenden "Passphrase" überprüft. Dies kann nur der Besitzer des "Private Key"!
   Der entschlüsselte Text steht in der Zwischenablage
6. Strg V oder ***Bearbeiten***: ***Einfügen*** auswählen. Der entschlüsselte Text steht jetzt im E-Mail
7. Rest wie gewohnt.

Unterschreiben

1. Text im E-Mail wie gewohnt schreiben,
2. zu unterschreibenden Text markieren
3. Strg C bzw. Strg X (wie oben)
4. PGP-Schaltstelle anklicken und
5. "Sign Clipboard" oder "Zwischenablage unterschreiben" auswählen (es ist die Passphrase als Bestätigung einzugeben, dass man diese Person auch ist),
6. Strg V es wird der Text mit der Unterschrift eingefügt.
7. E-Mail versenden

Unterschrift prüfen

1. E-Mail öffnen - wie gewohnt
2. Text und Unterschrift (wieder inklusive der Beginn- und Ende-Zeilen) markieren
3. Strg C
4. PGP-Schaltstelle anklicken und
5. "***Decrypt Clipboard***" oder "***Unterschrift prüfen***" auswählen
6. "Good Signature..." Unterschrift in Ordnung (Die Prüfung erfolgte anhand eines vorhandenen "Public Key", denn die Unterschrift muss zum "Private Key" des Unterschreibenden dazupassen)

(Eigenen) Public Key versenden

1. Im Schlüsselbund (Launch PGP-Keys) den zu exportierenden Schlüssel markieren und "Export" wählen.
2. Herausgelösten Schlüssel in einer Datei abspeichern (.asc-Datei)
3. Schüsseldatei xxx.asc als Anlage zum E-Mail versenden

Per E-Mail empfangenen Public Key hinzufügen

1. E-Mail wie gewohnt öffnen
2. Dateianlage (xxx.asc-Datei) doppelt anklicken
3. Fertig

Public Key als Text empfangen

1. E-Mail Öffnen
2. Public Key markieren und
3. Strg C
4. PGP-Schaltstelle anklicken und
5. "***Add Key from Clipboard***" auswählen
6. Fertig

Tipps

- Sichern Sie Ihr Schlüsselpaar mehrmals auf anderen Medien (Diskette, CD-ROM, ...). Geht es verloren, haben Sie keine Chance, es wiederherzustellen!
- Lesen Sie die einzelnen Schritte in der Hilfefunktion von PGP nach, wenn Sie nicht mehr wissen, wie es geht! Hier finden Sie auch noch weitere Dokumentation.
- Sie können PGP auch für andere Dinge verwenden als "nur" für s E-Mail. Benutzung analog zu obigen Schritten.

Was noch zur digitalen Signatur zu sagen wäre

Seit 1.1.2000 ist die digitale Signatur in Österreich der bisher üblichen manuellen Unterschrift rechtlich gleichgestellt. Damit können die üblichen Vorgänge des Geschäftsverkehrs auch elektronisch - z.B. via Internet - abgewickelt werden. Es gibt nur mehr 3 Gründe, die eine manuelle Unterschrift notwendig machen (Weg zum Notar):

1. Firmenbucheintrag
2. Grundstückskauf
3. Erbschaftsangelegenheiten / Mündelabhandlungen

Sie können das Signaturgesetz im Internet unter http://www.ris.bka.gv.at/ nachlesen.

Auch Behördenwege werden durch die Anwendung der digitalen Signatur vereinfacht werden. Verfolgen Sie die Entwicklung im Amtshelfer unter http://www.help.gv.at/.

Das Signaturgesetz sieht die Einrichtung sogenannter Signatur-Provider vor. Diese Provider müssen jede erdenkliche Maßnahme treffen, dass ein Missbrauch der Unterschrift oder des Verfahrens unterbunden wird. Sie haften mit ihrem Firmenvermögen dafür. Sie garantieren, dass Unterschriften auch wirklich von einer bestimmten Person geleistet wurden. Der Public Key steht am Server des Providers und daher kann jeder über diesen Server die Unterschrift prüfen gehen.

Der Provider hat - laut Signaturgesetz - die Identität des Antragstellers zu prüfen. Dies geschieht durch Ausweisleitung bei jedem österreichischen Postamt.

Es gibt verschiedene Sicherheitsstufen. Je nach Stufe wird eine andere jährliche Gebühr verrechnet. Lesen Sie mehr darüber beim Signatur-Provider a-sign http://www.a-sign.at/.

8 Literatur

Für die Erstellung dieses Skriptums wurden verschiedene Quellen, vor allem aus dem Internet benutzt. Im einzelnen wollen wir folgende Quellen erwähnen:

http://lbs.bw.schule.de/mmlfb/

Auf diesem Bildungsserver finden sich viele Skripten und Anleitungen zu den Themen

- Aufbau und Betrieb eines Internet-Servers
- Erstellen von Webpages mit HTML

Erich Schikuta, Internet - Theorie und Praxis. Powerpoint-Präsentation; Universität Wien, 1999.