

# **INTERNET - Möglichkeiten und Dienste**

# Table of Contents

<u>INTERNET - Möglichkeiten und Dienste</u> .....	1
<b>Internet</b> .....	<b>1</b>
<u>Inhalt</u> .....	1
<u>Internet - was ist das?</u> .....	1
<u>Internet-Dienste im Überblick</u> .....	2
<u>Internet-Zugang und E-Commerce</u> .....	2
<u>Kriminalität und Sicherheit im Internet</u> .....	2
<u>Intranet - Internet im Kleinen</u> .....	2
<u>Internet-Technik</u> .....	2
<u>Suchen im Internet</u> .....	2
<u>Anhang</u> .....	3
<u>INTERNET - Möglichkeiten und Dienste</u> .....	4
<b>1 INTERNET - Was ist das?</b> .....	<b>5</b>
1.1 <u>Entwicklung des Internet</u> .....	12
<u>Stephen Eick (Bell Labs) veröffentlichte einige Visualisierungen des</u> <u>Internet-Datenverkehrs ( <a href="http://www.bell-labs.com/user/eick/index.html">http://www.bell-labs.com/user/eick/index.html</a>)</u> .....	14
1.2 <u>Struktur</u> .....	14
1.3 <u>Verwaltung</u> .....	18
1.4 <u>Wie funktioniert das Internet</u> .....	25
1.5 <u>Dokumentation</u> .....	26
1.6 <u>Der Internet-Wurm</u> .....	28
1.7 <u>Zukunftstendenzen (Stand 2002)</u> .....	30
<u>INTERNET - Möglichkeiten und Dienste</u> .....	31
<b>2 Internet-Dienste im Überblick</b> .....	<b>31</b>
2.1 <u>Die elektronische Post</u> .....	32
<u>Weg eines normalen Briefes</u> .....	37
2.2 <u>News - öffentliche Diskussionsforen</u> .....	41
2.3 <u>Telnet</u> .....	42
2.4 <u>FTP (File Transfer Protocol)</u> .....	44
2.5 <u>SSH und SCP/SFTP</u> .....	44
2.6 <u>IRC (Internet Relay Chat)</u> .....	45
2.7 <u>WWW (World Wide Web)</u> .....	49
2.8 <u>Ping</u> .....	49
2.9 <u>Traceroute</u> .....	50
2.10 <u>Whois</u> .....	50
2.11 <u>Java, Javascript, VRML, Flash etc</u> .....	53
<u>INTERNET - Möglichkeiten und Dienste</u> .....	54
<b>3 Internet-Zugang und E-Commerce</b> .....	<b>54</b>
3.1 <u>Die verschieden Arten des Zugangs</u> .....	55
3.2 <u>Internet-Provider</u> .....	56
3.3 <u>Hardware, Software und Betriebssysteme</u> .....	58
3.4 <u>Verhalten im Internet</u> .....	59
3.5 <u>Kommerz im Internet</u> .....	62
3.6 <u>Die eigene Homepage</u> .....	63
<u>INTERNET - Möglichkeiten und Dienste</u> .....	64

# Table of Contents

<b>4 Kriminalität und Sicherheit im Internet</b> .....	<b>64</b>
4.1 Juristisches.....	64
Strafgesetzbuch:.....	66
4.2 Copyright-Probleme.....	66
4.3 Sicherheit.....	70
4.4 Schutz des Netzwerks durch Firewalls.....	73
4.5 Obscure URLs.....	74
INTERNET - Möglichkeiten und Dienste.....	75
<b>5 INTRANET - Internet im Kleinen</b> .....	<b>75</b>
Prolog.....	75
5.1 Inhouse-Kommunikation vereinfachen.....	76
5.2 Web-Publishing und Data Warehousing.....	76
5.3 Interaktion mit dem Benutzer.....	76
5.4 Vom Intranet zum Extranet.....	77
INTERNET - Möglichkeiten und Dienste.....	78
<b>6 Internet-Technik</b> .....	<b>78</b>
6.1 Denken in Schichten.....	79
6.4 Neuere Entwicklungen.....	82
INTERNET - Möglichkeiten und Dienste.....	83
<b>7 Suchen im Internet</b> .....	<b>83</b>
7.2 Wie funktionieren Suchmaschinen?.....	85
7.2 Erster Grundsatz beim Suchen.....	85
7.3 Wann lohnt sich die Suche im Internet?.....	86
7.4 Suchmaschinen versus Verzeichnisse.....	86
7.5 Suchmaschinen richtig bedienen.....	86
7.6 So gehen Sie bei der Suche vor.....	88
INTERNET - Möglichkeiten und Dienste.....	89
<b>8 Anhang</b> .....	<b>89</b>
8.1 Literaturempfehlungen.....	89
Online-Informationen.....	90
8.2 Domain name registries around the world.....	93
Bericht der Bundesregierung.....	94
INTERNET - Möglichkeiten und Dienste.....	95
<b>Kleiner E-Mail-Knigge</b> .....	<b>95</b>
Allgemeines.....	97
Regeln für Antwortmails (Zitieren).....	98
Attachments.....	98
Legenden und Hoaxes.....	99
E-Mail-Viren und SPAM.....	101
Was ist eigentlich Spam? Und was bedeutet ECP, EMP, UBE, UCE?.....	103
Phishing - Passwort-Fischer.....	104
Pharming.....	105
Weiterführende Links.....	106
INTERNET - Möglichkeiten und Dienste.....	106
SSH-Tunnel mit Putty.....	111
Copyright © FH München, FB 04, Prof. Jürgen Plate.....	112

# Table of Contents

<b><u>- JAVA EINBLICK -</u></b> .....	<b>112</b>
<u>Ein Referat von Antje König</u> .....	112
<u>Inhalt</u> .....	112
<u>Das ist Java</u> .....	113
<u>Das kann Java</u> .....	113
<u>Die Geschichte von Java</u> .....	113
<u>Hot Java / Netscape Navigator</u> .....	114
<u>Die Programmiersprache</u> .....	114
<u>Die Eigenschaften</u> .....	115
<u>Ein Beispielprogramm</u> .....	115
<u>Erklärung:</u> .....	115
<u>Kompilierung:</u> .....	117
<u>HTML Implementierung</u> .....	117
<u>Als Beispiel:</u> .....	117
<u>Erläuterung:</u> .....	117
<u>Attribute</u> .....	117
<u>Parameter</u> .....	118
<u>Bsp:</u> .....	118
<u>JDK - Java Development Kit</u> .....	119
<u>Kommerzialisierung?</u> .....	119
<u>"Eingriff in die Internet-Kultur</u> .....	119
<u>JavaScript</u> .....	120
<u>Syntax:</u> .....	120
<u>Auch hier ein Beispiel:</u> .....	120
<u>Quellenangaben / Literatur:</u> .....	121
<u>Die wichtigsten LINKS:</u> .....	title

# Internet

*"As a net is made up of a series of ties, so everything in this world is connected by a series of ties."*



If anyone thinks that the mesh of a net is an independent, isolated thing, he is mistaken.

It is called a net because it is made up of a series of interconnected meshes, and each mesh has its place and responsibility in relation to other meshes."

(Buddha)

## Inhalt:

### 1. Internet - was ist das?

1. Entwicklung des Internet
2. Struktur
3. Verwaltung
4. Wie funktioniert das Internet?
  1. Internet Protocol IP
  2. Transportprotokolle TCP und UDP
  3. Domain Name Service (DNS)
  4. Das Client-Server-Prinzip
5. Dokumentation
6. Der Internet-Wurm
7. Zukunftsperspektiven

### 2. Internet-Dienste im Überblick

1. Die elektronische Post
2. News - Öffentliche Diskussionsforen
3. Telnet
4. FTP (File Transfer Protocol)
5. SSH und SCP/SFTP
6. IRC (Internet Relay Chat)
7. WWW (World Wide Web)

8. Ping
9. Traceroute
10. Whois
11. Java, Javascript, VRML, Flash etc.

### 3. **Internet-Zugang und E-Commerce**

1. Die verschiedenen Arten des Zugangs
2. Internet-Provider
3. Hardware, Software und Betriebssysteme
4. Verhalten im Internet
5. Kommerz im Internet
6. Die eigene Homepage

### 4. **Kriminalität und Sicherheit im Internet**

1. Copyright-Probleme
2. Juristisches
3. Sicherheit
4. Firewalls
5. Obscure URLs

### 5. **Intranet - Internet im Kleinen**

1. Prolog
2. Inhouse-Kommunikation vereinfachen
3. Daten aufbereiten
4. Interaktion mit dem Benutzer
5. Vom Intranet zum Extranet

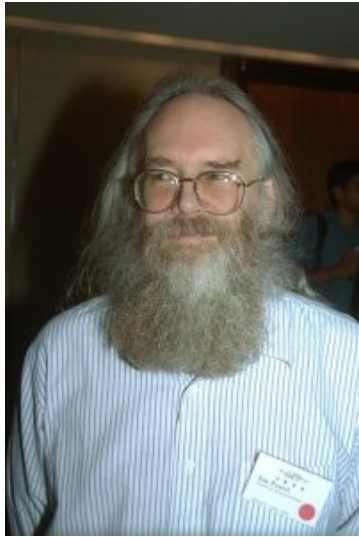
### 6. **Internet-Technik**

1. Denken in Schichten
2. TCP/IP
3. Höhere Protokolle
4. Neuere Entwicklungen

### 7. **Suchen im Internet**

### 8. **Anhang**

1. Literaturempfehlungen
  2. Domain name registries around the world
  3. Bericht der Bundesregierung über die Erfahrungen und Entwicklungen bei den neuen Informations- und Kommunikationsdiensten im Zusammenhang mit der Umsetzung des Informations- und Kommunikationsdienste-Gesetzes (IuKDG)
  4. TIPP: Kleiner E-Mail-Knigge
  5. TIPP: SSH-Tunnel mit Putty
  9. Skript als PDF (aus HTML konvertiert)
  10. Download des gesamten Skripts
-



**Jonathan Postel**, 55, "Gottvater des Internet" wurde er gern genannt, nicht nur seiner wehenden Haarpracht wegen. Postel war einer der Computernarren, die in den sechziger Jahren anfangen, ein weltweites Datennetz zu knüpfen. Und wenn es heute, mit Abermillionen angeschlossenen Rechnern, noch immer funktioniert, ist das zu einem guten Teil Jonathan Postel zu danken. Der zurückhaltende Mann, der am liebsten in Sandalen herumschlappte, war Herr über das ausgeklügelte Adreßsystem des Internet. Er vergab und verwaltete die Internet-Adressen. Und er tat das so effizient, daß dem Netz, selbst als es immer schneller wuchs, das drohende Chaos erspart blieb. Weil soviel von ihm abhing, galt er als einer der mächtigsten Männer der Netzwelt, aber auch als einer, dem man vertrauen konnte. Jonathan Postel starb am 16. Oktober 1998 in Santa Monica, Kalifornien, an den Folgen einer Herzoperation.

Unter

[http://www.uni-koeln.de/rrzk/kompass/80/wmwork/www/k80\\_9.html](http://www.uni-koeln.de/rrzk/kompass/80/wmwork/www/k80_9.html) findet sich ein längerer Nachruf von Vint Cerf.

---

*Copyright © Hochschule München, FB 04, Prof. Jürgen Plate*  
*Letzte Aktualisierung: document.write(document.lastModified);*



## INTERNET - Möglichkeiten und Dienste

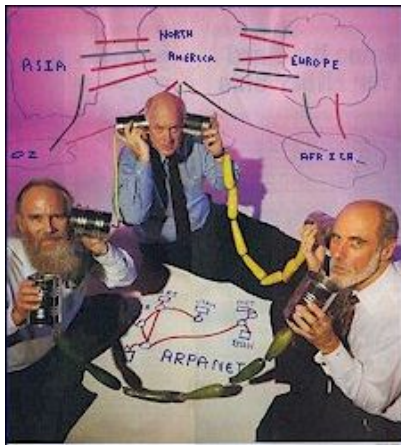
*Prof. Jürgen Plate*

---

# 1 INTERNET - Was ist das?

"Auf lange Sicht gesehen mag der Aspekt, die zwischenmenschliche Kommunikation zu fördern, sogar wichtiger werden als technische Ziele"  
Andrew S. Tanenbaum in seinem Buch 'Computer-Netzwerke'.

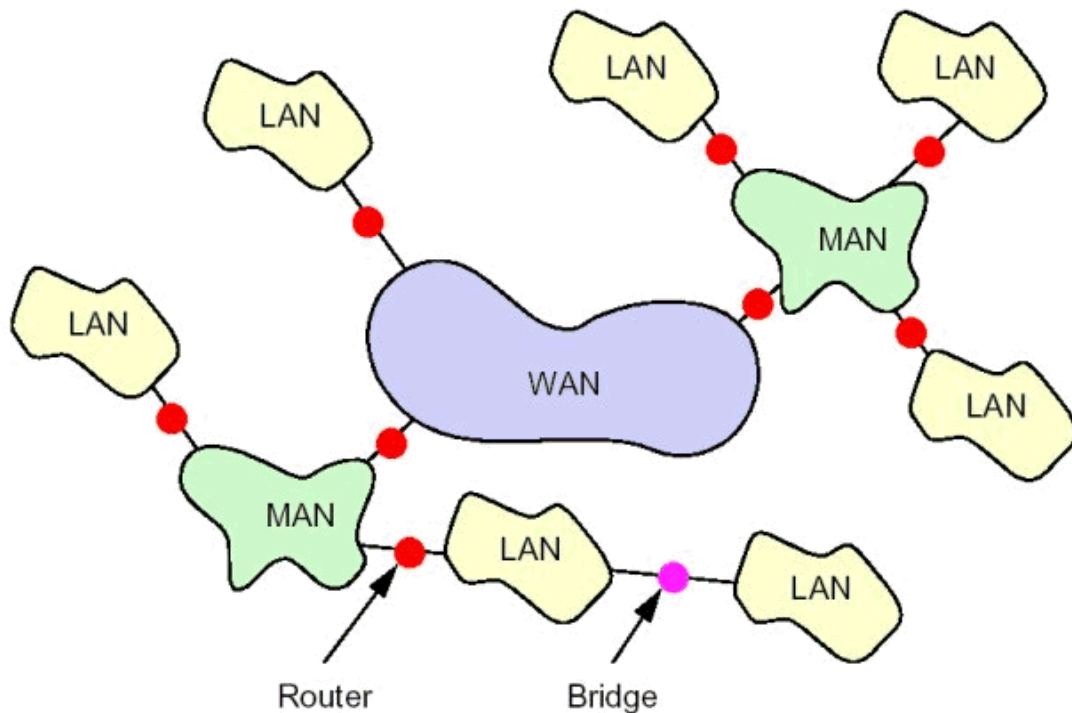
Das sogenannte 'Internet' ist in erster Linie eine technische Möglichkeit, mit vielen Partnern weltweit die unterschiedlichsten Informationen auszutauschen. Wie das genau geschieht, was technisch dahinter steckt und was man alles machen kann, soll nun ein wenig durchleuchtet werden.



Pioniere des Internet: Jon Postel, Steve Crocker und Vint Cerf (v.l.n.r.)

- Mit *Internet* bezeichnet man nur das spezielle Leitungsnetz, mit dem Computer auf der ganzen Welt miteinander verbunden sind, und das in diesem Leitungsnetz verwendete Netzwerkprotokoll *TCP/IP*. Als *Internet* wird somit die Verbindung aller Rechner bezeichnet, die über das TCP/IP-Protokoll (Transmission Control Protocol/Internet Protocol) miteinander kommunizieren.
- Im Internet werden die Informationen paketweise übertragen. So kann eine Leitung von mehreren Computern gleichzeitig verwendet werden (siehe später).
- Das Internet ist hardwareunabhängig. Je nach Leitungsart werden die Internet-Pakete z. B. in Ethernet-Pakete verpackt. *Gateways* sorgen für den Übergang von einer Leitungsart zu einer anderen.
- Im Internet sind alle Rechner gleichberechtigt, es gibt keine Unterschiede zwischen *Servern* (Dienstanbietern) und *Clients* (Dienstnehmern). Die Funktion hängt nur von der verwendeten Software ab.
- Die einzelnen Dienste des Internets werden durch *Portnummern* unterschieden (siehe später).

Das *Internet* ist also ein Verbund von kleineren Netzen - bis hinab zu einem lokalen Netz (LAN), das beispielsweise einer Firma gehört. Alle Rechner eines Netzes können mit allen Rechnern aller anderen am Internet angeschlossenen Netze kommunizieren. Durch den Anschluß weiterer Netze entsteht ein größeres Netz. Dies hat zu einer weltweiten Vernetzung von Rechnern mit TCP/IP geführt, die unter dem Namen *Internet* läuft. Es gibt jedoch niemanden, der für das Internet verantwortlich ist, vielmehr tragen die Betreiber der einzelnen Teilnetze Verantwortung für ihr Netz und die Verbindung zu einigen Nachbarn. Jeder erbringt freiwillig auch Leistungen für das gesamte Netz (z. B. Mail-Weiterleitung), die teils kostenlos sind, teils einer gegenseitigen Abrechnung der Leistungen unterliegen. Auf diese Weise kann man von jedem Rechner im Internet zu jedem anderen angeschlossenen Rechner gelangen.



Basis des Netzes bilden die Leitungen der verschiedenen Telekom-Gesellschaften auf der Welt, die ihre Leitungen oder Leitungskapazitäten für die Verbindung der einzelnen Netze vermieten. Aber nicht nur Firmen mieten Leitungen von den TK-Gesellschaften, sondern auch die sogenannten 'Internet-Provider'. Diese Provider bieten dann ihrerseits einen Internet-Zugang für Firmen oder Privatleute an. Später mehr dazu.

Oft wird das reine Transportmedium Internet mit seinen Anwendungen gleichgestellt, z. B. werden vielfach Internet und WWW als identisch betrachtet. Damit wird man diesem Medium aber nicht gerecht, denn es gibt viele Anwendungen, die das Internet nutzen, z. B. Elektronische Post (E-Mail), Dateiübertragung (FTP), Terminalzugriff auf ferne Rechner (Telnet), Diskussionsforen (News), Online-Diskussionen (Chat), Synchronisation der Uhrzeit, Internet-Telefonie und vieles mehr.

### 1.1 Entwicklung des Internet

Der erste Schritt in Richtung Internet wurde 1957 getan, als in den USA die *Advanced Research Projects Agency* (ARPA) des Verteidigungsministeriums gegründet wurde. Dies geschah als Reaktion auf den Abschub des ersten russischen Satelliten "Sputnik". Die ARPA hatte die Aufgabe, Technologien zu entwickeln, die für das Militär von Nutzen sind. Später wurde die ARPA in "Defense Advanced Research Projects Agency" (DARPA) umbenannt, da ihre Interessen primär militärischen Zwecken dienen sollten. Die ARPA war keine Organisation, die selbst forscht, sondern sie verteilte Aufträge an Universitäten und Forschungsinstitute.

Das Internet wurde vor etwa 20 Jahren aus einem dieser Forschungsprojekte des ARPA geboren. Das Ziel dieses experimentellen Projektes war, ein Netzsystem zu entwickeln, das auch partielle Ausfälle verkraften konnte. Kommunikation sollte immer nur zwischen einem Sender und einem Empfänger stattfinden. Das Netz dazwischen wurde als unsicher angesehen. Jegliche Verantwortung für die richtige Datenübertragung wurde den beiden Endpunkten der Kommunikation, Sender und Empfänger, auferlegt. Dabei sollte jeder Rechner auf dem Netz mit jedem anderen kommunizieren können.

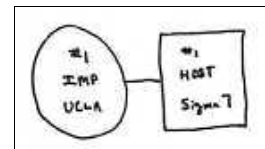
Um die geforderte Zuverlässigkeit eines nicht-hierarchischen Netzes zu erreichen, sollte das Netz als

## INTERNET - Möglichkeiten und Dienste

ein paketvermitteltes Netz (packet-switched network) gestaltet werden. Bei der Paketvermittlung werden zwei Partner während der Kommunikation nur virtuell miteinander verbunden. Die zu übertragenden Daten werden vom Absender in Stücke variabler oder fester Länge zerlegt und über die virtuelle Verbindung übertragen; vom Empfänger werden diese Stücke nach dem Eintreffen wieder zusammengesetzt. Im Gegensatz dazu werden bei der Leitungsvermittlung (circuit switching) für die Dauer der Datenübertragung die Kommunikationspartner fest miteinander verbunden. Hierzu entstand 1961 die "Paket Theorie" von Leonard Kleinrock. Dieses Verfahren wurde allerdings bei dem ersten Wide Area Network der Welt 1965 noch nicht angewandt. Hier wurden die Rechner TX-2 vom MIT und Q-32 von *System Development Corporation* in Santa Monica direkt verbunden.

Daraufhin wurde 1967 das erste Designpapier über das ARPANET von Lawrence G. Roberts veröffentlicht und ein Jahr später wird das Konzept der Paket-vermittelnden Netze der ARPA präsentiert.

Richtig begonnen hatte alles möglicherweise am 2. September 1969? An diesem Tag wurde im Labor von Leonard Kleinrock an der Universität von Kalifornien in Los Angeles (UCLA) der erste Computer an einen Interface Message Processor (IMP) angeschlossen. "Wir hielten das nicht gerade für einen historischen Moment", erinnerte sich Kleinrock gegenüber einem AP-Reporter. "Wir hatten nicht einmal eine Kamera dabei. Aber es war die Geburtsstunde des Internet". Der IMP war ein mächtiger Klotz von einem Spezialrechner, der nach militärischen Normen von der Firma Bolt, Beranek & Newmann (BBN) gebaut worden war. Seine einzige Aufgabe bestand darin, Daten zu senden und zu empfangen, den Empfang zu überprüfen und das Senden zu wiederholen, wenn etwas nicht geklappt hatte. Ein IMP sollte einem Computer vorgeschaltet sein und rund um die Uhr laufen können - eine beträchtliche Anforderung zu einer Zeit, in der Rechner jede Woche für einige Stunden gewartet werden mußten. Der Bau des IMP durch BBN erfolgte nach einer Ausschreibung der Forschungsabteilung im Verteidigungsministerium, die an 140 Firmen geschickt wurde. Damals führende Firmen wie IBM und Control Data lehnten die Ausschreibung als "nicht realisierbar" ab, nur die kleine BBN wagte es, die vier IMPs anzubieten. Sie wurden kurzerhand auf Basis eines Honeywell 516 von Grund auf neu konstruiert.



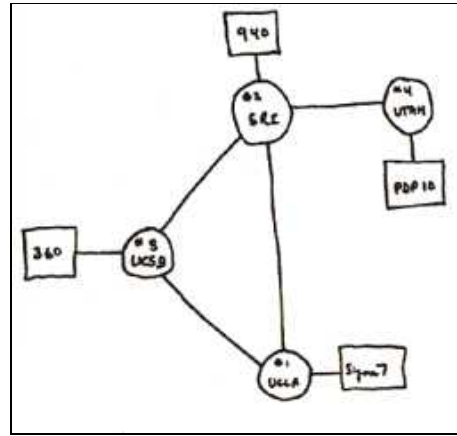
Frank Heart war der leitende Ingenieur beim Bau der IMPs: "Wir haben das Internet bei BBN überhaupt realisiert. Es ist wie mit Einstein. Der erzählt etwas von  $e=mc^2$  und die Leute vom Alamos Project bauen die Bombe", erklärte Heart gegenüber Reuters - auch die Nachrichtenagenturen halten sich an unterschiedliche Varianten.

Dennoch kann man den Bau eines IMP nicht ohne die Vorarbeit sehen. Den Anstoß zur Konstruktion der ganzen Netzwerktechnik gab Bob Taylor, ein Mitarbeiter der Advanced Research Projects Agency (ARPA). Er ärgerte sich über die Tatsache, daß er drei verschiedene Terminals brauchte, um mit drei Universitäten zu kommunizieren, an denen die ARPA militärische Grundlagenforschungen finanzierte. Sein Wunsch nach einer einheitlichen Kommunikation wurde von J.C.R. Licklider aufgenommen, der zusammen mit Bob Taylor das bahnbrechende Papier *The Computer as Communications Device* veröffentlichte. In ihm schimmerte erstmals die Idee der Vernetzung aller Computer auf. Danach brauchte es knapp sechs Jahre, bis die Grundlagenforschung so weit abgeschlossen war, um das Vernetzungsprojekt in die Tat umzusetzen.

## INTERNET - Möglichkeiten und Dienste

Als der erste gelieferte IMP am 2. September 1969 mit einem Computer in Kleinrocks Büro Daten austauschte, war die Geburt des Internet noch nicht ganz zu Ende. BBN mußte drei weitere IMPs liefern, die peu à peu in Stanford, Santa Barbara und Salt Lake City aufgestellt wurden. Zwischen dem Büro von Kleinrock und dem Stanford Research Institute wurde das erste *Ping* durch die Leitung geschickt. Danach entspann sich an jenem 10. Oktober 1969 ein bizarrer Dialog, den viele für die wahre Geburtsstunde des Internets halten. Kleinrock wollte sich über die beiden existierenden IMPs mit seinem Computer auf dem Computer in Stanford einloggen; dazu mußte er den Login-Befehl absetzen. "Wir tippten also das L ein und fragten am Telefon "Seht ihr das L?" "Wir sehen es", war die Antwort.

Wir tippten das O ein und fragten "Seht ihr das O?" "Ja, wir sehen das O!" Wir tippten das G ein ... und die Maschine stürzte ab." Doch ein paar Stunden später war der digitale Schluckauf behoben, der Versuch wurde wiederholt - und diesmal ging nichts schief: Zwischen Stanford und Los Angeles lief das erste funktionsfähige Wide-Area-Network (WAN): Das Internet war geboren.

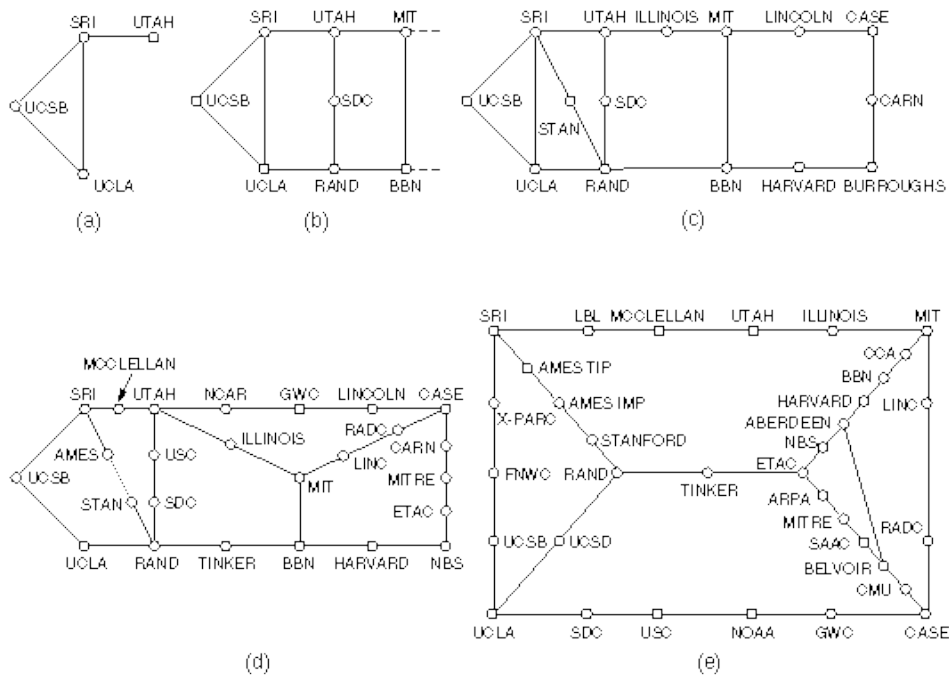


Ende 1969 wurde dann von der University of California Los Angeles (UCLA), der University of California Santa Barbara (UCSB), dem Stanford Research Institute (SRI) und der University of Utah ein experimentelles Netz, das ARPANet, mit vier Knoten in Betrieb genommen. Diese vier Universitäten wurden von der ARPA gewählt, da sie bereits eine große Anzahl von ARPA-Verträgen hatten. Keine andere technische Entwicklung in diesem Jahrhundert hat eine derartige Erfolgsgeschichte wie dieses inzwischen erdballumspannende Netzwerk, keine andere einen derart vielschichtig verzweigten Einfluß auf alle denkbaren Aspekte des gesellschaftlichen und privaten Lebens. Die Konturen des Internet

wurden erst 1971 sichtbar, als das Forschungsprojekt unter dem Namen ARPANet mit 15 IMPs erstmals der Öffentlichkeit vorgestellt wurde.

Erst zu diesem Zeitpunkt hatte das Netz ungefähr die Dimensionen, die in den ersten Netzskizzen des Informatikers Larry Roberts anno 1966 schon eingezeichnet waren, der die Idee des dezentral verknüpften Netzwerks entwickelte. Heute ist Roberts einer der Väter, die am stärksten gegen die Idee vom kriegssicheren Internet polemisieren: "Es ist ein Gerücht, daß das Internet entwickelt wurde, um einen nuklearen Krieg auszuhalten. Das ist total falsch. Wir wollten ein effizientes Netz aufbauen." Erst später sei das Argument eines Atomschlags hinzugekommen - das erwies sich beim Lockermachen weiterer Forschungsgelder als äußerst nützlich. Das ARPANet wuchs rasant und überspannte bald ein großes Gebiet der Vereinigten Staaten.

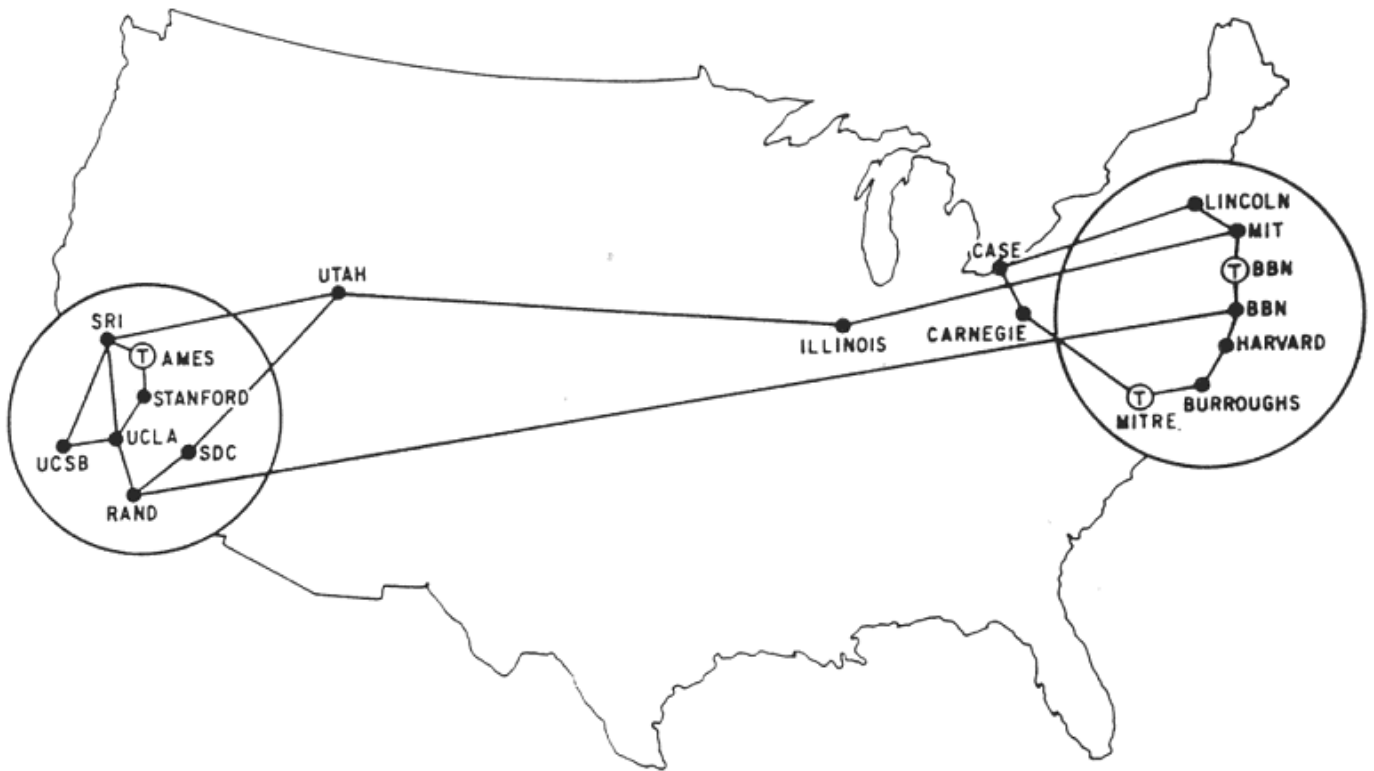
## INTERNET - Möglichkeiten und Dienste



Wachstum des ARPA-Net (Quelle: A. S. Tanenbaum: Computernetworks)

- a. Dezember 1969
- b. July 1970
- c. März 1971
- d. April 1971
- e. September 1972

## INTERNET - Möglichkeiten und Dienste

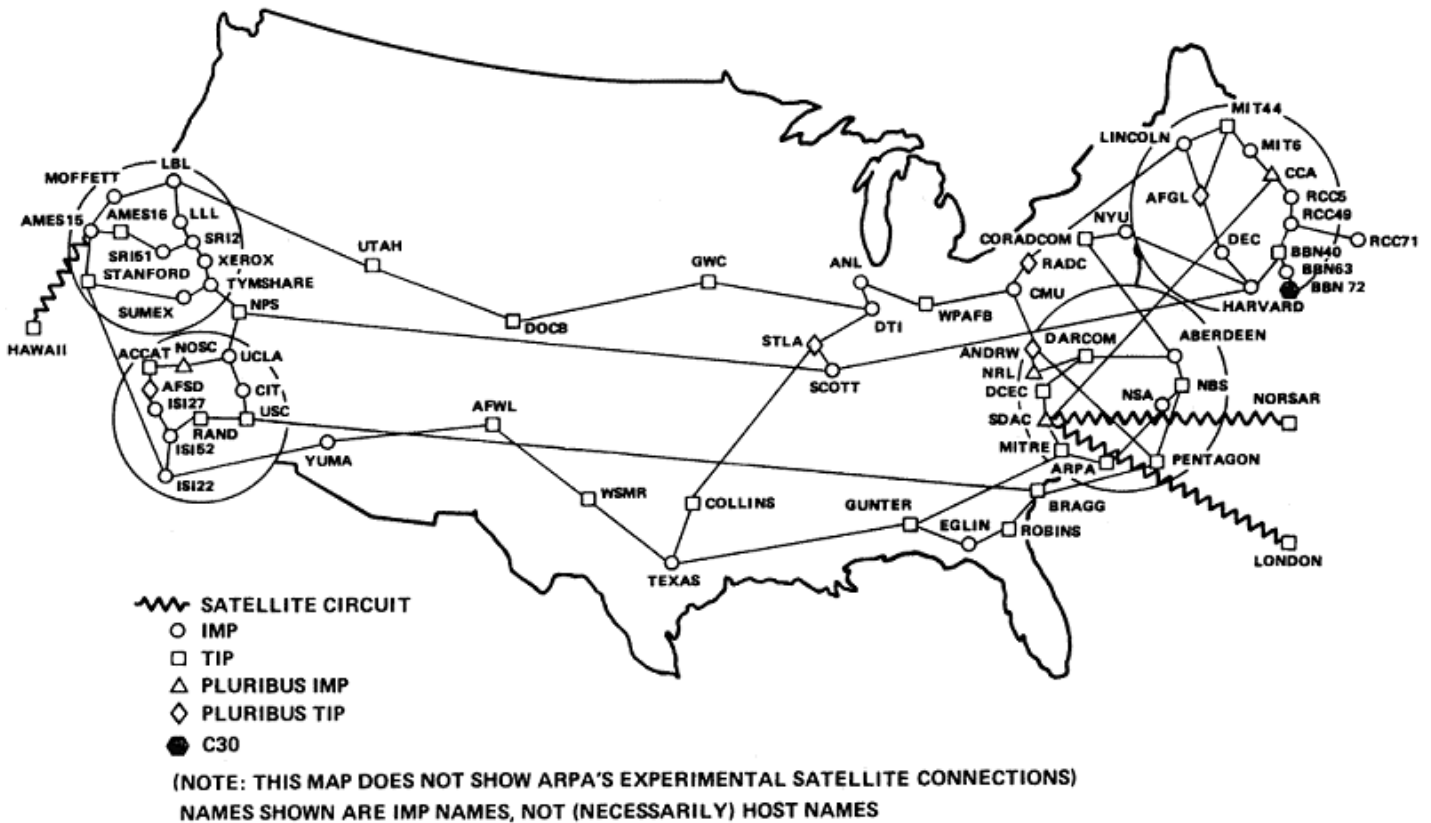


September 1971

Anfang der Siebziger kam die Idee auf, daß die IMPs von Computern abgelöst werden könnten, die keine Spezialrechner waren. Im Jahre 1972 beschäftigte sich der Xerox-Informatiker Bob Metcalfe damit, das hausinterne Netzwerk MAXC an das ARPANet zu hängen. Dabei erfand er eine Übertragungstechnik, die er Ethernet nannte. Zeitgleich wurde der erste "Request for Comment" (RFC) veröffentlicht. Der Inhalt ist *Host Software*. Im Laufe der nächsten Jahre wurden immer mehr Rechner an das ARPANET angeschlossen, 1973 die Universität "Collage of London". Dies war die erste internationale Anbindung an das ARPANET.

Die Erfindung erregte das Interesse von Bob Kahn und Vint Cerf, die 1974 den ersten Vorschlag für ein einheitliches Rechnerprotokoll machten: "A Protocol for Paket Network Intercommunication". Dieses Papier beschreibt im Detail das Design des "Transmission Control Protocols" (TCP). Dieses Protokoll wurde TCP/IP genannt und am 1. Januar 1983 in den Rang eines offiziellen Standards erhoben: Viele Netzwerker halten denn auch dieses Datum für den offiziellen Geburtstag des Internet.

## ARPANET GEOGRAPHIC MAP, OCTOBER 1980



Selbst heute, 30 Jahre später, ist die Bedeutung der kulturtechnischen Leistung "Internet" erst in Umrissen erahnbar. Der weitere Ausbau verlief langsam und gemächlich, auch nach mehr als 10 Jahren arbeiteten gerade mal rund 200 Systeme (Hosts) im ARPA-Net zusammen. Schon zu diesem Zeitpunkt war das ARPA-Net kein Netzwerk wie jedes andere auch, sondern definierte eine Kommunikationsstruktur. Jeder Host im ARPA-Net konnte ein Zentralcomputer in einem lokalen Netzwerk sein, so daß das ARPA-Net ein Netzwerk aus Netzwerken bildete eben ein "Internet". Dieses Internet wucherte unaufhaltsam weiter und allmählich beschleunigte sich das Wachstum und nahm einen exponentiellen Verlauf. Im Oktober 1984 zählte man rund 1000 Hosts, 1987 waren es etwa 10000 und 1989, zwei Jahre später, über 100 000.

Mit der Zeit und dem Wachstum des ARPA-Net wurde klar, daß die bis dahin gewählten Protokolle nicht mehr für den Betrieb eines größeren Netzes, das auch mehrere (Teil)Netze miteinander verband, geeignet war. Aus diesem Grund wurden schließlich weitere Forschungsarbeiten initiiert, die 1974 zur Entwicklung der TCP/IP-Protokolle führten. TCP/IP wurde mit der Zielsetzung entwickelt, mehrere verschiedenartige Netze zur Datenübertragung miteinander zu verbinden. Da etwa zur gleichen Zeit an der University of California an einem neuen Betriebssystem mit Namen UNIX entwickelt wurde, beauftragte die (D)ARPA die Firma Bolt, Beranek & Newman (BBN) und die University of California at Berkeley zur Integration von TCP/IP in UNIX. Dies bildete auch den Grundstein des Erfolges von TCP/IP in der UNIX-Welt. Ein weiterer Meilenstein beim Aufbau des Internet war die Gründung des NSFNET der National Science Foundation (NSF) Ende der achtziger Jahre, die damit fünf neu gegründete Super Computer Centers den amerikanischen Hochschulen zugänglich machte. Dies war ein wichtiger Schritt, da bis zu diesem Zeitpunkt Super Computer nur der militärischen Forschung und einigen wenigen Anwendern sehr großer Firmen zur Verfügung standen.

## INTERNET - Möglichkeiten und Dienste

Parallel zu den Entwicklungen im ARPANet und NSFNET arbeitete die ISO (International Standards Organisation) seit den achtziger Jahren an der Standardisierung der Rechner-Kommunikation. Die Arbeiten mündeten in der Definition des ISO/OSI Referenzmodells. Die Entwicklung entsprechender OSI-Protokolle und -Anwendungen gestaltete sich aber als ein äußerst zäher Prozeß, der bis heute nicht als abgeschlossen anzusehen ist. Hersteller und Anwender konnten darauf natürlich nicht warten und so wurde die Internet Protokoll-Familie TCP/IP im Lauf der Zeit in immer mehr Betriebssystemen implementiert. TCP/IP entwickelte sich so unabhängig von den offiziellen Standardisierungsbestrebungen zum Quasi-Standard.

Im Jahr 1983 wurde das ARPA-Net schließlich von der Defence Communications Agency (DCA), welche die Verwaltung des ARPA-Net von der (D)ARPA übernahm, aufgeteilt. Der militärische Teil des ARPA-Net, wurde in ein separates Teilnetz, das MILNET, abgetrennt, das durch streng kontrollierte Gateways vom Rest des ARPA-Net - dem Forschungsteil - separiert wurde. Nachdem TCP/IP das einzige offizielle Protokoll des ARPA-Net wurde, nahm die Zahl der angeschlossenen Netze und Hosts rapide zu. Das ARPA-Net wurde von Entwicklungen, die es selber hervorgebracht hatte, überrannt. Das ARPA-Net in seiner ursprünglichen Form existiert heute nicht mehr, das MILNET ist aber noch in Betrieb.

Das Jahr 1989 markiert einen Wendepunkt. Zum einen wurde zum 20. Geburtstag des ARPA-Net seine Auflösung beschlossen - es ging in das 1986 gegründete Netzwerk der National Science Foundation (NSF) über - zum anderen schrieb Tim Berners-Lee am Genfer Kernforschungszentrum CERN ein Diskussionspapier mit dem Titel "Information Management: A Proposal", mit dem er den Kommunikationsprozeß am CERN verbessern wollte. Aus diesem Vorschlag entwickelt sich in den nächsten Monaten das "World Wide Web" (WWW). Das System leistete erheblich mehr als geplant - es entpuppte sich als als das einfachste, effizienteste und flexibelste Verfahren, um beliebige Informationen im Internet zu publizieren. Die Einführung des WWW sorgte für den bis dato kräftigsten Wachstumsschub des Internet. Dauerte es von 1969 bis 1989 immerhin 20 Jahre, bis mehr als 100 000 Hosts zusammengeschlossen waren, so waren es 1990 bereits über 300000 und 1992 wurde die Millionengrenze überschritten. Der Durchbruch und die selbst erfahrene Netzveteranen überraschende explosionsartige Verbreitung des Internet und des WWW setzte 1993 ein, als Marc Andreessen sein Programm "Mosaic herausbrachte, mit dem auch der unizeschulte Computerlaie auf früher kryptische Kommandos und ein erhebliches Spezialwissen nötig war, genügte nun ein einfacher Mausclick. Aus Mosaic wurde ein Jahr später Netscape und - "the rest is history".

Keiner der ARPANet-Entwickler war sich bewusst, mit seiner Arbeit ein wichtiges Stück Technikgeschichte zu schreiben. Alle waren sie damit befasst, knifflige technische oder programmiertechnische Probleme zu lösen. Mitunter waren es sogar persönliche Probleme: Len Kleinrock schilderte seine Version des Aufkommens von E-Mail als erste illegale Nutzung der neuen Technik. Kleinrock entdeckte im September 1973, daß er seinen Rasierer in England vergessen hatte. Dort fand eine Konferenz über das ARPANet statt, die er vorzeitig verlassen mußte. Kleinrock setzte sich an ein Terminal und stellte eine Verbindung zu einem Konferenzteilnehmer her, der gerade online war. Zwei Tage später war der Rasierer bei ihm. Und schon 1972 führte Ray Tomlinson den Klammeraffen @ als Teil der User-Adressen eines Programms ein, mit dem sich Nachrichten verschicken ließen - einfach deswegen, weil er das Zeichen auf seinem 33-Tasten-Keyboard sonst am wenigsten benötigte.

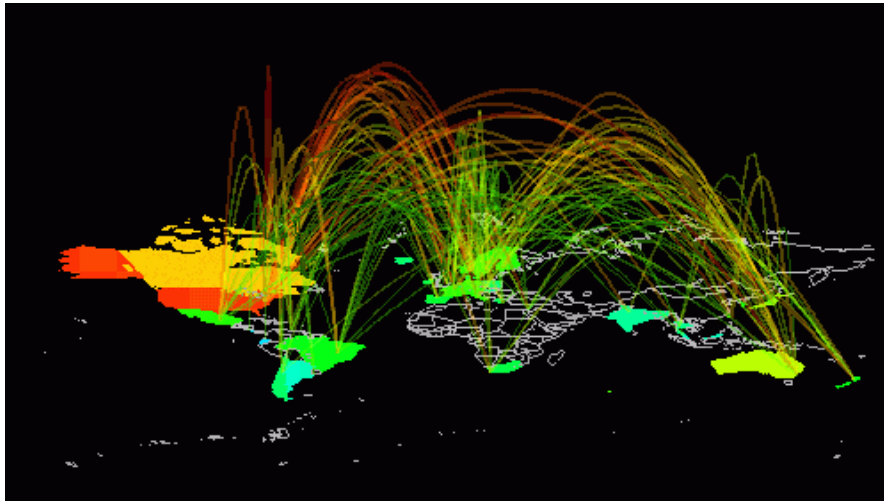
Im Jahre 1998 lud die Internet Society die Protagonisten der ersten Stunde zu einem Panel mit dem hübschen Titel *Unexpected Outcomes of Technology, Perspectives on the Development of the Internet*. Alle Beteiligten bekundeten in fröhlicher Einigkeit, daß sie die Idee eines weltumspannenden Kommunikationsnetzes für alle Erdenbürger bis Anfang der 90er für eine Idee von Verrückten gehalten hätten. "Man muß es einfach so sehen: Wir waren von unserem Netzwerk überzeugt. Wir haben unverdrossen nach Lösungen gesucht und waren damit erfolgreich. Außenstehende mögen uns für verrückt gehalten haben. Wir fanden eher, das wir positiv plemplem waren", erklärte Jon Postel in einem seiner letzten Interviews. Er muß es wissen: Ist er doch auch einer der Väter des Internet und

## INTERNET - Möglichkeiten und Dienste

war bis zu seinem Tod lange Jahre verantwortlich für die RFCs (Request for Comments), in denen die Internet-Standards festgeschrieben sind.

Die Genialität, die man den Entwicklern des Internet aus heutiger Sicht zuschreibt, wird von den Technikern eher spöttisch kommentiert. Ken Klingenstein, der für die Simplizität des von ihm entwickelten SNMP (Simple Network Management Protocol) geehrt wurde, klärte den genialen Wurf im Interview auf: "Mir kam die Idee zu SNMP in einer Bar auf dem Weg nach Hause. Ich nahm die Serviette des Drinks und schrieb alle Befehle auf. Es mußten einfach wenige sein, weil die Serviette so klein war."

Ähnlich war es um TCP/IP bestellt: Vint Cerf brachte eine der ersten Skizzen zum Kommunikationsprotokoll der Internet-Welt auf der Rückseite der Bedienungsanleitung seines Hörgeräts zu Papier. In einer Forschungsgruppe befaßt sich der PR-erfahrene Cerf inzwischen publikumswirksam mit dem transgalaktischen Protokoll: dem technischen Problem, wie die langen Laufzeiten von Datenpaketen bei der Kommunikation zwischen Mars und Erde optimal überbrückt werden können.



**Stephen Eick (Bell Labs) veröffentlichte einige Visualisierungen des Internet-Datenverkehrs (<http://www.bell-labs.com/user/eick/index.html>)**

In den 70er Jahren wurden auch die ersten Dienste für das ARPANET entwickelt. Im Jahr 1971 entwickelte von Ray Tomlinson das erste Programm für den E-Mail-Dienst. Es basierte auf einem rechnerinternen Mail-Programm und einer experimentellen FTP-Version. Ray ist auch verantwortlich für die Verwendung des "@". Erst sechs Jahre später wurde E-Mail erstmals im RFC 733 spezifiziert. 1979 kam Kevin MacKenzie auf die Idee, Emotionen im Text auszudrücken. Hierzu erfand er die ersten Smilies :-)

Ein Jahr nach dem ersten E-Mail-Programm wurde Telnet im RFC 318 spezifiziert. Wieder ein Jahre später gab es dann die Standardisierung des "File Transfer Protocol" im RFC 454. Etwa gleichzeitig wurde der RFC 741 geschrieben, in dem die Spezifikation des "Network Voice Protocol" stand. Auf der Basis dieser Dienste und dem Versuch des ARPANETs gibt BBN 1974 "Telenet" frei, eine kommerzielle Version des ARPANETs. Es ist das erste kommerzielle, paketorientierte Netz.

1982 entsteht durch die Implementierung der TCP/IP-Protokollfamilie und deren Einsatz im ARPANET der Begriff "Internet". Ein Jahr später kommen Workstations mit Berkley UNIX 4.2 (BSD) auf den Markt, dem ersten UNIX mit eingebauter TCP/IP-Unterstützung. Im darauffolgenden Jahr wird das Name-Server-Konzept entworfen und 1984 eingeführt. Die erste registrierte Domain war 1985 `symbolics.com`. Zu dieser Zeit gab es schon über 1000 Hosts.

Stephen Eick (Bell Labs) veröffentlichte einige Visualisierungen des Internet-Datenverkehrs (<http://www.bel>

## INTERNET - Möglichkeiten und Dienste

1986 wurde das *Nation Science Foundation Network* (NSFNET) gegründet. Es hatte eine Backbone-Geschwindigkeit von 56 KBit/s und verband vorwiegend Universitäten und dazugehörige Institutionen. Dieses Netz wurde in den darauffolgenden Jahren ständig erweitert. 1988 wird das Backbone auf T1-Leitung (1,544 MBit/s) erweitert und 1989 wird auch Deutschland an das NSFNET angeschlossen. Durch den Erfolg des NSFNET stieg auch die Zahl der Hosts im Internet auf 1987 über 10000. Zwei Jahre später waren es dann schon über 100.000.

Durch das starke Wachstum wurde 1991 das Backbone des NSFNET auf T3 (44,736 Mb/s) erweitert. Die Kapazität überschreitet erstmals 1 Billionen Bytes bzw. 10 Milliarden Pakete pro Monat. Auch die Anzahl der Hosts übersteigt 1992 erstmals die 1.000.000 Marke.

Auch 1991 veröffentlichte CERN das von Tim Berners-Lee entwickelte World-Wide Web (WWW). Der spätere Gründer von Netscape, Marc Andreessen, war der Entwickler des 1993 veröffentlichten Browsers namens "Mosaic".

Heute werden "World Wide Web" und "Internet" vielfach synonym gebraucht und die Größe des Internets verdoppelte sich alle 12 bis 18 Monate. Die neuesten Schätzungen gehen von über 43 Millionen angeschlossenen Systemen aus, die Anzahl der Menschen, die Zugriff auf Informationen im Internet haben, wird auf über 160 Millionen geschätzt, davon sind etwa 36 Millionen in Europa. In Deutschland ermittelte 1999 die GfK 8,4 Millionen. Allerdings sind derartige Zahlen und Erhebungen nur mit großer Vorsicht zu genießen. Schon die technische Messung der Hostzahlen ist alles andere als trivial und in hohem Maße interpretationsbedürftig. Nur eines ist wirklich sicher: Das Internet und das WWW breiten sich seit Jahren mit schwindelerregender Geschwindigkeit aus.

Wer mehr über die Geschichte des Internets erfahren möchte, sollte Hobbes' Internet Timeline, lesen. Dieses Dokument wurde 1998 als RFC 2235 veröffentlicht.

Zum Wachstum des Internet in Deutschland siehe: <http://www.nic.de/Netcount/netStatHosts.html>

Weitere Quellen zur Geschichte des Internet:

- Internet Society - ISOC: History of the Internet
- Musch J.: Die Geschichte des Netzes: ein historischer Abriss
- Hauben M.: Behind the Net: The Untold History of the ARPA-Net and Computer Science
- Hauben R.: The Birth and Development of the ARPA-Net
- Pioniere des Internet
- Marco Siegert: Das Internet - Grundlagenwissen für die Polizei

Weiter Karten zur Ausdehnung des ARPA-Netzes:

- April 1971
- August 1971
- September 1973
- Juni 1974
- März 1977
- Connectivity Map 1991 von Larry Landweber
- Connectivity Map 1997 von Larry Landweber
- Infos von Telegeography
- Automatisch generierte Backbone-Karten
- BT Backbone Maps
- Studie Deutschland Online

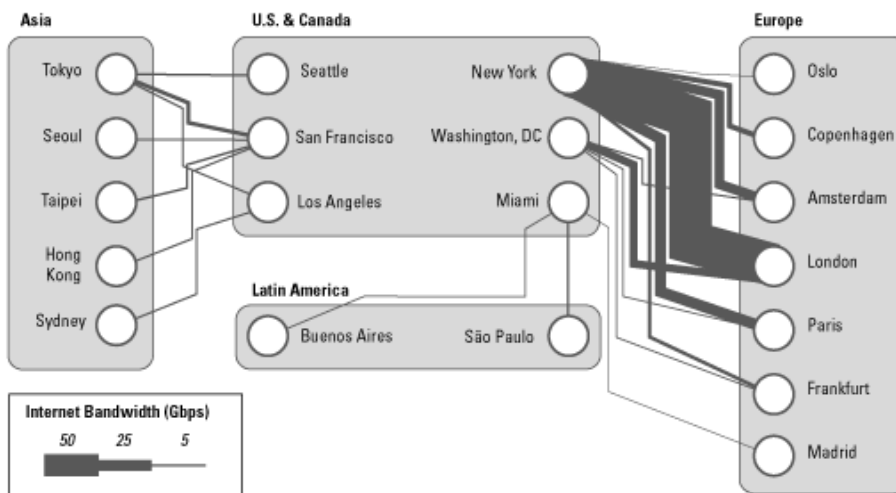
Für Kaffeetrinker ist auch noch der RFC 2324 (erschieden 1. April 1998) interessant. Er handelt vom *Hyper Text Coffee Pot Control Protocol (HTCPCP/1.0)*.

Stephen Eick (Bell Labs) veröffentlichte einige Visualisierungen des Internet-Datenverkehrs <http://www.bel>

## 1.2 Struktur

Das Internet, wie es sich heute darstellt, ist ein Geflecht aus vielen tausenden von Netzen und Millionen von Hosts. Eine aktuelle Statistik für Europa findet man beim deutschen Network Information Center ([www.nic.de](http://www.nic.de)).

Diese an das Internet angeschlossenen Rechner sind in der Regel in lokale Netze (LAN = Local Area Network) eingebunden. Organisatorisch zusammengehörende LANs sind zumeist in regionalen Netzwerkverbunden organisiert, welche wiederum mindestens einen überregionalen Zugang besitzen, den WAN- (Wide Area Network) Anschluß. Das weltumspannende Internet bietet so ein homogenes Erscheinungsbild, obwohl es technisch auf einem heterogenen Konglomerat an Netzwerken aufgebaut ist.



© 2002 TeleGeography, Inc.

### Schema der wichtigsten Internetverbindungen (Die Liniendicke ist proportional der Bandbreite)

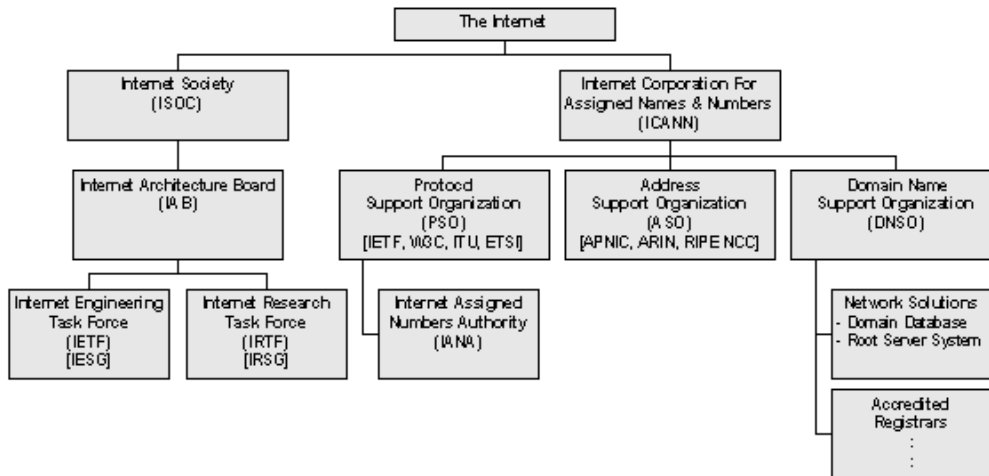
Die Frage, wer nun zum Internet gehört und wer nicht, ist schwer zu beantworten. Bis vor einigen Jahren war die Antwort, daß jedes Gerät, welches die TCP/IP-Protokolle beherrschte und Verbindung zum 'Rest der Welt' hatte, zum Internet zu zählen war. Inzwischen wurden in anderen großen Netzwerken (Bitnet, DECnet, ...) Methoden entwickelt, um Daten mit dem Internet über sogenannte Gateways auszutauschen. Diese Techniken wurden inzwischen derart verfeinert, daß Übergänge zwischen diesen Netzwelten und dem Internet für den Benutzer teilweise vollkommen transparent vorstatten gehen. Offiziell ist nicht geklärt, ob diese Netze nun zum Internet gehören oder nicht. Ein Rechner wird allgemein dann als zum Internet gehörend angesehen, wenn:

- er mit anderen Rechnern über TCP/IP kommunizieren kann
- er eine Netzadresse (IP-Nummer, siehe unten) besitzt
- er mit anderen Rechnern kommunizieren kann, die eine Netzadresse haben

## 1.3 Verwaltung

Es erhebt sich natürlich die Frage, wer im Internet bestimmt, wie was gemacht wird. Dazu gibt es keinen Präsidenten oder Direktor sondern allgemein anerkannte Arbeitskreise, die ihre Mitglieder aus der Benutzerschaft rekrutieren. Die Entscheidungen dieser Versammlungen werden von den Internet-Anwendern als verbindlich akzeptiert. Es steht jedem frei, ebenfalls an der Entwicklung des Internet mitzuarbeiten. Dies führt insbesondere dazu, daß Firmen sich in diese Arbeitskreise einbringen, um möglichst früh die Weichen 'richtig' stellen zu können.

## INTERNET - Möglichkeiten und Dienste



Die **ISOC**, die Internet Society, ist die Dachorganisation untergeordneter netzbezogener Organisationen. Sie umfasst mehrere Hundert Organisationen und eine lange Reihe von Privatpersonen und ist aufgeteilt in Unterorganisationen (Chapters), z. B. nach Themen oder Regionen. Sie richtet die alljährliche Internetkonferenz aus und kümmert sich beispielsweise auch darum, daß der Begriff 'Internet' ein frei verfügbarer Begriff wird und nicht als Wortmarke oder sonst wie geschützter Begriff in das Eigentum von Privatpersonen übergeht. Die ISOC befasst sich mit:

- dem Wachstum und der Entwicklung des weltweiten Internet
- der Art, wie das Internet benutzt wird und werden kann
- sozialen, politischen, und technischen Fragen im Zusammenhang mit dem Internet

Die ISOC ernennt die Mitarbeiter des IAB, die der Nominierungs-Ausschuss des IETF vorschlägt.

Das **IAB** (Internet Architecture Board) ist das höchste Gremium im Internet. Es segnet Entscheidungen über Standards und Adressvergabe ab und läßt diese Entscheidungen bekanntgeben. Es dokumentiert die gültigen Protokolle des Internet, ernennt die Mitglieder der **IESG** (Internet Engineering Steering Group) und setzt die Vorsitze der IANA (Internet Assigned Numbers Authority) ein. Außerdem leitet es das RFC-System, mit dem die Fortschreibung der Protokolle und Richtlinien des Internet realisiert wird. Alle Entscheidungen, die das IAB trifft, werden in den sogenannten *Request for Comments* (RFC) veröffentlicht. Das IAB umfasst zwei spezialisierte Untergruppen, die *Internet Engineering Task Force* (IETF) und die *Internet Research Task Force* (IRTF). Diese beiden Gremien sind für die Weiterentwicklung und Definition der kurz- und mittelfristigen Internet-Protokolle und -Architekturen für die Bereiche Applikationen, Host- und Benutzerservice, Internet-Service, Routing, Adressierung, Netzwerkmanagement, Operations, Security und OSI-Integration verantwortlich. Sie erarbeiten die für das IAB zum Entscheid notwendigen Grundlagen. Das IAB ist eine technische Beratungsgruppe der ISOC. Seine Verantwortungen schliessen ein:

- IESG Auswahl: Das IAB ernennt den IESG Vorsitzenden und die Mitarbeiter der IESG, die der Nominierungs-Ausschuss der IETF vorschlägt.
- Architekturübersicht: Das IAB stellt eine Übersicht der Architektur der Protokolle und Verfahren bereit, die vom Internet benutzt werden.
- Massstäbe für Entwicklung und Dokumentation: Das IAB stellt Verfahren für das Erarbeiten von Internet-Standards bereit. Es nimmt auch Beschwerden wegen schlechter Umsetzung der Standards entgegen.
- RFC-Serien und IANA: Das IAB ist verantwortlich für das redaktionelle Management und die Veröffentlichung der *Request for Comments* (RFC) Dokument-Serien, und für die Verwaltung der verschiedenen *Internet Assigned Numbers* (IAN, Zuordnung der IP-Adressen).
- Das IAB handelt als Vertreter der Interessen der *Internet Society* an Besprechungen mit anderen Organisationen betreffend Standards und anderen technischen und organisatorischen

## INTERNET - Möglichkeiten und Dienste

Fragen im Zusammenhang mit dem Internet.

- Beratung der ISOC: Das IAB berät das ISOC in Fragen rund um das Internet, die technischer, architektonischer, verfahrensmässiger, und (wo angemessen) politischer Natur sind.

Die **IANA** (Internet Assigned Numbers Authority), deren Vorstand J. Postel war, ist zuständig für alle eindeutigen Ressourcen im Netz, also Netzadresse, Domainnamen und Portnummern.

Technische und betriebliche Probleme werden zuvor in der **IETF** (Internet Engineering Task Force) behandelt, eine offene Vereinigung von Administratoren, Technikern, Forschern und Softwareproduzenten, die die Weiterentwicklung von Protokollen, Sicherheitsrichtlinien, Routing etc. des Internet betreibt. Ihre Treffen sind für jedermann offen. Sie fördert auch den Technologie- und Wissenstransfer zwischen der **IRTF** (Internet Research Task Force) und leistet somit Vermittlung und Koordination zwischen Forschung und Praxis (wobei auch der zeitliche Rahmen eine Rolle spielt: während die IETF kurz- und mittelfristig die Standards definiert, ist die Aufgabe der IRTF die langfristige Kursbestimmung und Forschung).

Die Standards werden dann in sogenannten RFCs (Request for Comments) niedergelegt. Das **ISC** (Internet Software Consortium) ist zuständig für die Referenzimplementierung der zentralen Internetprotokolle.

Standards von Protokollen oder sonstigen netzrelevanten Vereinbarungen können an die zuständigen Gruppen der IETF, ISOC oder inzwischen auch der ICANN eingereicht werden, welche dann die Probleme je nach betreffendem Fachgebiet in lokale Arbeitsgruppen (Working Groups, WGs) weitergeben. Die anstehende Standardisierung wird als Internet Draft bezeichnet und hat vorerst überhaupt keine Geltungsmacht. Die Erörterung des Themas und die Einigung auf die besten Möglichkeiten finden über Mailinglisten statt. Treffen werden jährlich mehrmals organisiert, in denen dann auf Konsensebene die Ergebnisse zusammengefasst werden und in die RFC's eingehen. Trotz der inzwischen häufigen Zugehörigkeit der Mitglieder zu Industrieunternehmen wiegt technische Angemessenheit, Kompetenz und Engagement mehr wiegt als das Vertreten von Konzerninteressen. Ebenso ist eine starke 'Dienstaltershierarchie' feststellbar. Leute wie Cerf oder Kleinrock, die als 'Väter' des Internet gelten, genießen in Kreisen von Netztechnikern hohes Ansehen und werden eher wahrgenommen. Deutlich erkennbar ist auch die allgegenwärtige Verehrung des inzwischen verstorbenen Jon Postel, der die längste Zeit das RFC-System administriert hat. Die IETF wird in folgende acht funktionale Gebiete eingeteilt:

- Anwendungen (Applications)
- Internet
- IP Next Generation
- Netzwerkmanagement (Network Management)
- Betriebliche Auflagen (Operational Requirements)
- Routing
- Sicherheit (Security)
- Transport- und Anwenderdienste (Transport and User Services)

Die **Internet Engineering Steering Group** (IESG) ist verantwortlich für das technische Management der IETF-Aktivitäten und für die Internet Standards. Im Rahmen des ISOC verwaltet sie den Prozess gemäss den Regeln und Verfahren, die von den ISOC Trustees ratifiziert worden sind. Die IESG ist direkt verantwortlich für die Handlungen, die mit Eintragung in und Ausführung der Internet-Standards verbunden werden, einschliesslich abschliessender Zustimmung von Spezifikationen als Internet Standards.

Die **Internet Research Steering Group** (IRSG) "steuert" die Arbeiten der IRTF. Die Mitgliedschaft der IRSG beinhaltet den Vorsitzenden des IRTF, die Vorsitzenden der verschiedenen Forschungsgruppen und möglicherweise einzelne weitere Personen der Forschungsgemeinschaft (*members at large*).

## INTERNET - Möglichkeiten und Dienste

Ziel der **Internet Research Task Force** (IRTF) ist die Förderung der Forschung im Hinblick auf das Wachstum und die Zukunft des Internets. Dazu werden kleine langfristige Forschungsgruppen gebildet, die auf gezielten Forschungsgebieten, wie Internet Protokolle, Applikationen, Architektur und Technologie arbeiten. Folgende Forschungsgruppen sind derzeit gebildet:

- End-to-End
- Information Infrastructure Architecture
- Privacy and Security
- Internet Resource Discovery
- Routing
- Services Management
- Reliable Multicast

Die IRTF wird im RFC 2014 vollständig beschrieben.

Die **Internet Assigned Numbers Authority** (IANA) ist die zentrale Koordinationsstelle für die Zuweisung von eindeutigen Parameterwerten für Internet-Protokolle. Das heisst, sie ist für die Vergabe von IP-Adressen und Domain-Namen verantwortlich.

In der Vergangenheit, wurden die Aktivitäten der IANA durch die Regierung der USA unterstützt. Dies ist nun nicht mehr möglich oder angemessen. Die USA haben nicht vor, in der Zukunft weiter (Geld-)Mittel bereitzustellen und so muss sich die IANA auf ihre Organisationen verlassen können. Das Internet ist von einem Forschungsnetz für Hochschulen zu einem multimedialen Netz für die Allgemeinheit geworden, das von Leuten über alle Welt benutzt wird. Diese Veränderung in Funktion und in der Anwenderbasis fordert nach einer neuen standfesten Institution mit einer breiten Gemeinschaftsvertretung aller Benutzer.

Dieses neue IANA ist zur Zeit gerade im Begriff zu entstehen. Das alte IANA stand noch unter der Leitung von Dr. Jon Postel vom Information Sciences Institute der University of Southern California. Das neue IANA heisst **Internet Corporation for Assigned Names and Numbers** (ICANN) und wird als Non-Profit-Organisation von einem internationalen Verwaltungsrat bestehend aus Repräsentanten einer Wählerschaft und weiteren internationalen Repräsentanten geführt.

Mit der **ICANN** (Internet Corporation for Assigned Names and Numbers), wurde eine Organisation neuen Typs geschaffen, die den Anspruch hat, supranational und demokratisch zu funktionieren und die Schnittbereiche zwischen Internet und nationalen und internationalen Rechtsräumen zu regulieren. Während der populärste Gegenstand der Steuerung der IETF IP6 ist, schneidet sich die bekannteste Aufgabe der ICANN, nämlich die Vergabe von Domännennamen (insbesondere Top Level Domains), mit bestehenden Gesetzen wie Marken- und Urheberrecht. Diese Situation ist als solche nicht unvermeidlich, der Diskurs dreht sich im Allgemeinen aber nicht mehr um das 'ob', sondern das 'wie' der Umsetzung des Marken- und Urheberrechts im Internet.

Das **W3C** (World Wide Web Consortium) kümmert sich um die verbindlichen Standards des HTTP (HyperText Transfer Protocol), über welches Webseiten transferiert werden, und um die Weiterentwicklung des HTML-Standards. Im Unterschied zu staatlich unterstützten Gremien wie der ISO haben sich die angeführten Gremien selbst gebildet und sind nicht staatlich legitimiert. Das Konsortium bietet Informationen über das WWW und Standards für Entwickler und Benutzer, Referenzcode und -Implementationen, um die Standards zu umzusetzen und zu befördern, verschiedene Prototypen und Beispiel-Anwendungen, um den Gebrauch der neuen Technologie zu demonstrieren.

Das Konsortium wird geführt durch Tim Berners-Lee, Direktor und Erfinder des World Wide Web, und Jean-François Abramatic, als Chairman. W3C wird durch Mitgliedsorganisationen unterstützt und ist firmenneutral. Es erarbeitet mit der Web-Gemeinschaft gemeinsam Produktespezifikationen und Referenzsoftware, welche weltweit frei zur Verfügung gestellt wird.

Als ausführende Institutionen arbeiten sogenannte **NICs** (Network Information Centers) und **NOCs**

## INTERNET - Möglichkeiten und Dienste

(Network Operation Centers), welche auf weltweiter, kontinentaler, nationaler und regionaler Ebene existieren. Die Aufgabe des NIC ist die Vergabe und Koordination von eindeutigen Adressen und Namen im Internet. z. B. vergibt das zentrale InterNIC in USA ganze Adressbereiche an das europäische NIC (das RIPE-NCC (Reseaux IP Europeens - Network Coordination Center), welches seinerseits die deutsche Organisation, das DE-NIC, mit einem Teil dieses Adressbereiches beglückt. Das DE-NIC hat dann die Möglichkeit, eigenständig aus diesem Bereich Adressen zu vergeben, z. B. an einen Provider, der die Adressen an seine Endbenutzer weiterverteilt.

Die NOCs kümmern sich um den Betrieb des Netzes. Dazu gehören die Konfiguration der Netzkomponenten, die Behebung von Netzfehlern und die Beratung und Koordination der Netzteilnehmer.

Mitglied der IETF oder der ISOC kann prinzipiell jeder werden, Zugangsschwellen sind weniger die Zugehörigkeit zu Wirtschafts- oder Regierungsinstitutionen als vielmehr Expertenstatus und Engagement.

### 1.4 Wie funktioniert das Internet

Die Funktionsweise des Internet wurde bereits grob skizziert.

#### 1.4.1 Internet Protocol IP

Hier soll kurz erklärt werden, wie die zu übertragenden Informationen im Internet von einem auf den anderen Rechner kommen. Daten werden im Internet paketweise übertragen. Man spricht daher von einem paketvermittelten Netz. Zur Veranschaulichung ein Beispiel:

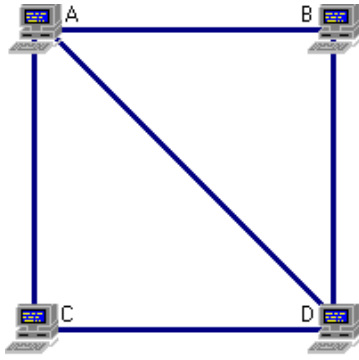
Im Telefonnetz wird für jedes Gespräch eine Leitung zwischen zwei Gesprächspartnern benötigt. Diese Leitung bleibt auch belegt, wenn keine Information übertragen wird, also keiner spricht. Hier handelt es sich um ein leitungsvermitteltes Netz.

Daten werden im Internet paketweise übertragen, d. h. längere Datenströme werden in kleinere Einheiten, eben die Pakete, zerlegt. Der Vorteil ist unter anderem, daß sich Pakete verschiedener Absender zeitlich hintereinander über eine Leitung schicken lassen.



Die Übertragung erfolgt fast so, wie Pakete von der Post transportiert werden. Wenn Informationsübertragung ansteht, wird ein Paket gepackt und mit einer Adresse versehen. Sodann wird dieses Informationspaket dem Netz überlassen, indem man es am Schalter abgibt. Das örtliche Postamt entscheidet dann aufgrund der Empfängeradresse, ob das Paket direkt an den Empfänger (wenn dieser also im Versorgungsbereich dieses Postamtes wohnt) auszuliefern ist, oder durch Einschalten von mehr oder weniger Zwischenstationen. In der Regel findet das Paket dann ein Postamt, das die Auslieferung an den Empfänger aufgrund der Adresse vornehmen kann. Schwierigkeiten bei der Auslieferung können dem Absender aufgrund der Absendeadresse mitgeteilt werden. Die einzelnen Teilnetze des Internet sind durch Geräte verbunden, die 'Router' genannt werden. Diese übernehmen die Funktion von Vermittlungsstellen und der ausliefernden 'Postämter'. Das folgende Beispiel-'Internet' verbindet vier Netze miteinander:

## INTERNET - Möglichkeiten und Dienste



- Wenn Rechner direkt miteinander verbunden sind (wie hier z. B. **A** mit **D**), so kommunizieren sie direkt miteinander.
- Wenn Rechner nicht direkt miteinander verbunden sind (wie z. B. **B** mit **C**), so wird die Kommunikation unter Verwendung von *Routern* (hier **D** oder **A**) abgewickelt. In diesem Fall sucht sich jedes Paket selbständig den schnellsten Weg.
- Wenn ein Router ausfällt, gelangen die Datenpakete auf Ausweichwegen zum Ziel. Möchte z. B. **A** mit **D** kommunizieren, und die Leitung **A - D** fällt aus, so werden die Daten über **B** oder **C** geroutet.
- Eine zweifelsfreie Identifizierung des Dienstnehmers durch den Dienstanbieter ist ohne zusätzliche Autorisierungsmechanismen nicht möglich: Wenn z. B. **B** ein Paket zu **C** versendet, muß das Paket **A** (oder **D**) passieren. **C** empfängt also das Paket von **A** und bekommt von **A** einen Hinweis, daß das Paket ursprünglich von **B** kam. Wenn **A** lügt, hat **C** keine Möglichkeit, dies zu überprüfen, da **C** nicht direkt mit **B** kommunizieren kann.
- Datensicherheit ist nicht gewährleistet, da jeder Rechner, der Pakete weiterleitet, diese Pakete auch mitlesen kann.

In den Adressen stecken Anteile, die das Empfänger-Postamt charakterisieren (Postleitzahl, Ort) und Anteile, die den Empfänger im Bereich dieses Postamtes festlegen. Diese Art der Informationsübertragung hat große Parallelen zur paketvermittelten Kommunikation im Internet. Die Adressen, die im Internet verwendet werden, bestehen aus einer 32 Bit langen Zahl. Damit sich die Zahl leichter darstellen läßt, unterteilt man sie in 4 Bytes (zu je 8 Bit). Diese Bytes werden dezimal notiert und durch Punkte getrennt (a.b.c.d). Zum Beispiel:

```
141.84.101.2  
129.187.10.25
```

Bei dieser Adresse werden zwei Teile unterscheiden, die Netzwerkadresse und die Rechneradresse, wobei unterschiedlich viele Bytes für beide Adressen verwendet werden:

Die Bereiche für die Netzwerkadresse ergeben sich durch die Zuordnung der ersten Bits der ersten Zahl (a), die eine Erkennung der Netz-Klassen möglich machen.

Netz-Klasse	Netzwerkadresse	Host-Adresse	Bereich binär
A	a b.c.d	1 - 126	01xxxxxx
B	a.b c.d	128 - 191	10xxxxxx
C	a.b.c d	192 - 223	11xxxxxx

Die Netzadressen von 224.x.x.x bis 254.x.x.x werden für besondere Zwecke verwendet, z. B. 224.x.x.x für Multicast-Anwendungen.

Grundsätzlich gilt:

## INTERNET - Möglichkeiten und Dienste

- Alle Rechner mit der gleichen Netzwerkadresse gehören zu einem Netz und sind untereinander erreichbar.
- Zur Koppelung von Netzen unterschiedlicher Adresse wird ein Router benötigt.
- Je nach Zahl der zu koppelnden Rechner wird die Netzwerkkategorie gewählt.

Jedes Datenpaket steckt quasi in einem 'Umschlag', der Absende- und Empfängeradressen enthält. Diese Adressen-Information wird den Nutzdaten vorangestellt, so daß jede Komponente im Netz, die das Protokoll TCP/IP beherrscht, aus dem Anfang des Datenpaketes herauslesen kann, woher das Paket kommt und wohin es soll. Komponenten, die das können und die zusätzlich die Möglichkeit haben, Datenpakete auf verschiedenen Wegen weiterzuschicken, sind die obengenannten Router. Diese nehmen von den Adressen immer erst die Netzanteile und entscheiden, ob das Netz direkt angeschlossen ist oder, falls nicht, an welchen nächsten Router es zu schicken ist.

Ein weiterer großer Vorteil des IP-Protokolls ist seine Unabhängigkeit vom tatsächlichen Datentransport. Die Datenpakete können über ein Ethernet, eine serielle Modemverbindung oder ein anderes Medium laufen. Für serielle Verbindungen, die häufig für die letzten Kilometer bis zum heimischen Rechner verwendet werden, gibt es spezielle IP-Protokolle. Angefangen hat es mit SLIP (Serial Line Internet Protocol), das heute weitgehend durch PPP (Point to Point Protocol) abgelöst ist. Das Internet Protocol IP ist also hauptverantwortlich dafür, daß Daten den richtigen Weg im Internet finden. Wenn ein Datenpaket nur korrekt in einen 'IP-Briefumschlag' gesteckt wird, kann es beruhigt dem Netz übergeben werden. Was aber ist, wenn mal ein Datenpaket verloren geht? Wie versendet man überhaupt mehr Daten als die maximale Paketgröße von 1500 Bytes? Was passiert, wenn auf einer größeren Maschine, die mehrere Benutzer gleichzeitig haben kann, Datenpakete für verschiedene Benutzer eintreffen? Hierfür gibt es die Transportprotokolle TCP und UDP.

### 1.4.2 Transportprotokolle TCP und UDP

Innerhalb jedes IP-Briefumschlages befindet sich nun ein weiterer Briefumschlag, der vom Transportprotokoll geschrieben wird. In den meisten Fällen handelt es sich dabei um TCP. Auf diesem Umschlag steht die Information, die auf die obengenannten Probleme eingeht. Im TCP- Briefumschlag befinden sich dann endgültig die zu übertragenden Daten.

Falls man also eine große Menge an Daten zu übertragen hat, wird diese in Pakete gestückelt und die Pakete mit Nummern versehen. Die Nummern stehen dann auf dem TCP-Paket, damit die Information auf der Empfängerseite wieder richtig zusammengehängt werden kann. Vom Empfänger muß für jedes Paket eine Empfangsbestätigung geschickt werden, damit der Sender weiterarbeiten kann. Fehlt die Empfangsbestätigung für eine Nummer, so wird dieses Paket nach einer gewissen Zeit noch einmal gesandt. Weiter berechnet TCP eine Prüfsumme, die ebenfalls auf das TCP-Paket geschrieben wird. Der Empfänger berechnet ebenfalls die Prüfsumme und nimmt das Paket nur an, wenn er zum selben Ergebnis wie der Sender kommt. Verfälschte oder verlorengegangene IP-Pakete werden also auf der TCP-Ebene überwacht und gegebenenfalls wiederholt. So wird sichergestellt, daß alle Daten korrekt und vollständig übertragen werden.

Was aber, wenn der Zielrechner nicht erreichbar ist? Dazu gibt es auf dem IP-'Paketaufkleber' ein Byte namens 'Time to live' (TTL). Jeder Router, über den das Paket läuft, vermindert diesen Wert um eins. Wird der Wert Null, dann wirft der nächste Router das Datenpaket weg. Auch diese Weise wird verhindert, daß unzustellbare Pakete im Netz herumgeistern. Der Absender bekommt keine Fehlermeldung. Er kann aber aus der Tatsache, daß nach einer angemessenen Wartezeit keine Empfangsbestätigung kommt, schließen, daß der Empfänger nicht erreichbar ist. Schließlich gibt es noch eine Eigenschaft zur Unterscheidung von TCP-Paketen.

In einem der folgenden Kapitel wird Ihnen eine Auswahl von Internet-Diensten vorgestellt. Es kann also durchaus vorkommen, daß mehrere Programme oder auch Benutzer über dieselbe Verbindung zweier Rechner miteinander kommunizieren wollen. Einzelne Verbindungen zwischen zwei Programmen oder zwei Benutzern werden durch sogenannte 'Portnummern' gekennzeichnet, die auch auf dem TCP-Paket hinterlegt sind. Mit dieser Information können Daten für verschiedene Programme oder Benutzer auf derselben Maschine oder Netzverbindung unterschieden werden. Etliche dieser Portnummern sind fest bestimmten Diensten zugeordnet und können nicht für andere Zwecke

## INTERNET - Möglichkeiten und Dienste

verwendet werden. Es gibt jedoch noch genügend freie Portnummern, die für neue Dienste oder spezielle Anwendungen von Standarddiensten verwendet werden können.

Diese und weitere Eigenschaften von TCP, die hier darzustellen zu sehr ins Detail führen würde, machen das Verfahren der Datenübertragung allerdings auch relativ aufwendig. Außerdem können (z. B. durch Warten auf die Empfangsbestätigung) durch TCP auch Verzögerungen auftreten. Es gibt nun Fälle, in denen sich der Aufwand nicht lohnt, und stattdessen eine schnelle Übertragung wichtiger ist. Für diese Fälle gibt es das Transportprotokoll UDP. Hier existieren keine Empfangsbestätigungen. Die Anwendung, also das Programm, das UDP benutzt, muß damit fertig werden, wenn gesendete Daten nicht ankommen. Dafür können die Daten ohne großen Aufwand beliebig schnell ins Netz hinausgeschoben werden.

In Kapitel 6 wird noch genauer auf die Protokolle und den Datentransport eingegangen.

### 1.4.3 Domain Name System (DNS)

In den vorigen Abschnitten wurde erklärt, wie Information im Internet von einem auf das andere Gerät, ja vom einzelnen Anwendungsprogramm zum korrekten Partner findet. Es mag vielleicht noch nicht ganz klar geworden zu sein, was der einzelne (menschliche) Benutzer von Internet- Diensten nun tatsächlich tun muß, und was die Protokolle für ihn automatisch tun. Nun, in der Regel startet der Benutzer ein Anwendungsprogramm für einen Internet-Dienst und gibt gleichzeitig eine Zieladresse (eines mehr oder weniger entfernten) Rechners an. Protokollintern, z. B. die Absendeadresse, die Paketierung usw., werden automatisch eingefügt.

Es hat sich ziemlich früh herausgestellt, daß menschliche Benutzer die numerischen IP-Adressen nicht benutzen wollen, sondern aussagekräftige und vor allem merkbare Namen bevorzugen. Außerdem ist es ein großer Nachteil der IP- Adressen, daß aus ihnen keinerlei geographische Information zu entnehmen ist. Man sieht einer Zieladresse nicht an, ob sie in Australien oder im Nebenzimmer lokalisiert ist, außer man kennt zufällig die gewählten Zahlen. Es wurde daher das Domain Name System entwickelt, das den Aufbau von Rechnernamen regelt. Es ordnet jedem (weltweit eindeutigen) Namen eine IP-Adresse zu. Dabei gibt es einige Varianten. Eine Maschine mit einer IP-Adresse kann mehrere Funktionen haben und daher auch mehrere Namen, die auf diese Funktionen hinweisen. Genauso kann eine Maschine (z. B. ein Router) viele IP-Adressen haben aber nur einen Namen.

Die Namen im DNS sind hierarchisch aufgebaut. Das gesamte Internet ist in Domains aufgeteilt, welche wieder durch Subdomains strukturiert werden. In den Subdomains setzt sich die Strukturierung fort. Diese Hierarchie spiegelt sich im Namen wieder. Die entsprechenden Domains werden durch Punkt getrennt. Beispiele:

mail.e-technik.fh-muenchen.de

ftp.microsoft.com Die Top-Level Domain (im Beispiel: de) steht ganz rechts und wird durch den Country-Code abgekürzt (weitere Beispiele: 'at' für Österreich, 'au' für Australien, 'fr' für Frankreich, 'uk' für Großbritannien, ... ). In den USA gibt es aus historischen Gründen allerdings sechs Top Level Domains (außer 'us', was sehr selten benutzt wird):

Generische TLDs	
com	Kommerzielle Organisationen
edu	(education) Schulen und Hochschulen
gov	(government) Regierungsinstitutionen
mil	militärische Einrichtungen
net	Netzwerk betreffende Organisationen
org	Nichtkommerzielle Organisationen

## INTERNET - Möglichkeiten und Dienste

int	Internationale Organisationen
arpa	und das alte ARPA-Net bzw. Rückwärts-Auflösung von Adressen

Ende 2000 sind neue TLDs von der ICANN genehmigt worden:

<b>Generische TLDs</b>	
pro	Ärzte, Rechtsanwälte und andere Freiberufler
biz	Business (frei für alle)
info	Informationsanbieter (frei für alle)
name	Private Homepages (frei für alle, aber nur dreistufige Domains der Form <Vorname>.<Name>.name)
<b>Generische, geförderte TLDs</b>	
aero	Luftfahrtindustrie
coop	Firmen-Kooperationen
museum	Museen
jobs	Stellenangebote
travel	Reisen

Unterhalb der Top-Level Domain treten dann Domains wie 'fh-muenchen' auf, die sich im Rahmen ihrer Organisationen auf diesen Namen geeinigt haben müssen, wie auch über die weitere Strukturierung des Namensraumes, etwa daß Fachbereiche einen Subdomain-Namen bilden (z. B. e-technik). Diese werden wieder strukturiert durch die Namen der einzelnen Lehrstühle und Institute. Als letztes Glied wird der einzelne Rechner mit seinem Hostnamen spezifiziert.

Für die Aufnahme einer Verbindung zwischen zwei Rechnern muß in jedem Fall der Rechnername in eine zugehörige IP- Adresse umgewandelt werden. Aus Sicherheitsaspekten ist es manchmal wünschenswert, auch den umgekehrten Weg zu gehen, nämlich zu einer sich meldenden Adresse den Namen und damit die organisatorische Zugehörigkeit offenzulegen.

Kennt man die Domänenadresse eines Rechners, dann hängt man diese einfach an den Usernamen mit einem At-Zeichen '@' dahinter, z. B.:

`meier@mail.e-technik.fh-muenchen.de` Ein kleiner Vergleich mit einer 'konventionellen' Adresse soll das verdeutlichen.

Stefan Meier	entspricht dem Benutzerpseudonym (meier)
bei Huber	entspricht dem Rechner (mail)
Beispielweg 5	entspricht der (Sub-) Domain (e-technik)
81234 München	entspricht der (Sub-) Domain (fh-muenchen)
West-Germany	entspricht der (Toplevel-) Domain (de)

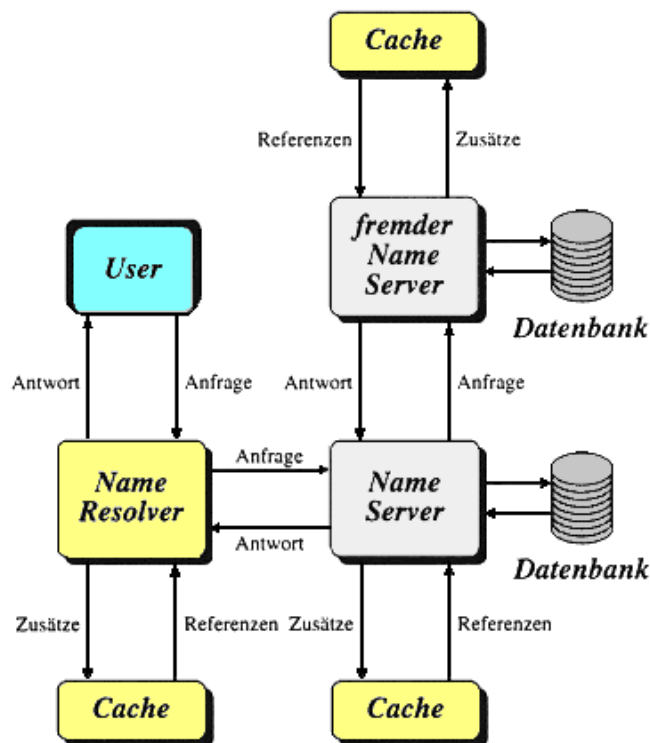
Damit das DNS funktioniert muß es Instanzen geben, die Namen in IP-Adressen und IP-Adressen in Namen umwandeln ('auflösen') können. Diese Instanzen sind durch Programme realisiert, die an größeren Maschinen ständig (meist im Hintergrund) im Betrieb sind und 'Nameserver' heißen. Jeder Rechner, der an das Internet angeschlossen wird, muß die Adresse eines oder mehrerer Nameserver wissen, damit die Anwendungen auf diesem Rechner mit Namen benutzt werden können. Die Nameserver sind für bestimmte Bereiche, sogenannte 'domains' oder 'Zonen', zuständig (Institute, Organisationen, Regionen) und haben Kontakt zu anderen Nameservern, so daß jeder Name aufgelöst

werden kann.

## Komponenten des DNS

Insgesamt sind es drei Hauptkomponenten, aus denen sich das DNS zusammensetzt:

1. Der **Domain Name Space**, ein baumartig, hierarchisch strukturierter Namensraum und die Resource Records. Das sind Datensätze, die den Knoten zugeordnet sind.
2. **Name Server** sind Programme bzw. Rechner, die die Informationen über die Struktur des Domain Name Space verwalten und aktualisieren. Ein Nameserver hat normalerweise nur eine Teilsicht des Domain Name Space zu verwalten. Oft wird auch der Rechner, auf dem das Nameserverprogramm läuft, als 'Nameserver' oder 'DNS-Server' bezeichnet.
3. **Resolver** sind die Programme, die für den Client Anfragen an den Nameserver stellen. Resolver sind einem Nameserver zugeordnet; bei Anfragen, die er nicht beantworten kann (anderer Teilbereich des Domain Name Space), kann er aufgrund von Referenzen andere Nameserver kontaktieren, um die Information zu erhalten.



Die Baumstruktur des DNS soll nun im weiteren untersucht werden. Ausgehend von der Wurzel (Root) folgen die Toplevel Domains. Diese Toplevel Domains spalten sich in weiteren Unterdomains auf.

Der **Nameserver** des DNS verwaltet also einzelne Zonen, die einen Knoten im DNS-Baum und alle darunterliegenden Zweige beinhalten. Auf jeder Ebene des DNS-Baums kann es Nameserver geben, wobei jeder Nameserver seinen nächsthöheren und nächstniedrigeren Nachbarn kennt. Aus Sicherheitsgründen gibt es für jede Zone in der Regel mindestens zwei Nameserver (*primary* und *secondary*), wobei beide die gleiche Information halten. Nameservereinträge können nicht nur die Zuordnung Rechnername - IP-Adresse enthalten, sondern (neben anderem) auch weitere Namenseinträge für einen einzigen Rechner und Angaben für Postverwaltungsrechner einer Domain (MX, mail exchange).

Basis des Nameservice bilden die "Root-Nameserver", die für die Top-Level-Domains zuständig sind. Die Mehrheit dieser Server ist in den USA beheimatet:



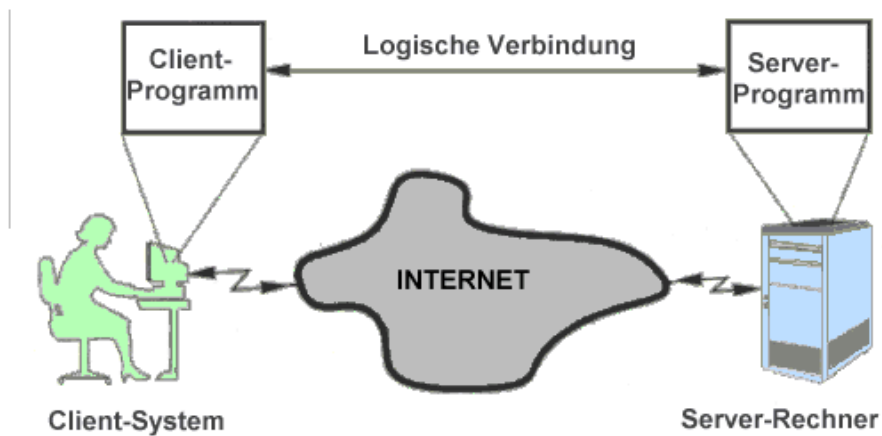
Name	Typ	Betreiber	URL
a	com	InterNic	<a href="http://www.internic.org">http://www.internic.org</a>
b	edu	ISI	<a href="http://www.isi.edu">http://www.isi.edu</a>
c	com	PSINet	<a href="http://www.psi.net">http://www.psi.net</a>
d	edu	UMD	<a href="http://www.umd.edu">http://www.umd.edu</a>
e	usg	NASA	<a href="http://www.nasa.gov">http://www.nasa.gov</a>
f	com	ISC	<a href="http://www.isc.org">http://www.isc.org</a>
g	usg	DISA	<a href="http://nic.mil">http://nic.mil</a>
h	usg	ARL	<a href="http://www.arl.mil">http://www.arl.mil</a>
i	int	NordUnet	<a href="http://www.nordu.net">http://www.nordu.net</a>
j	( )	(TBD)	<a href="http://www.iana.org">http://www.iana.org</a>
k	int	RIPE	<a href="http://www.ripe.net">http://www.ripe.net</a>
l	( )	(TBD)	<a href="http://www.iana.org">http://www.iana.org</a>
m	int	WIDE	<a href="http://www.wide.ad.jp">http://www.wide.ad.jp</a>

#### 1.4.4 Das Client-Server-Prinzip

Die meisten der Internet-Anwendungen funktionieren nach dem Client-Server-Prinzip. Deshalb soll auf diese Funktionsweise kurz eingegangen werden. Im einfachsten Fall kommunizieren dabei zwei Rechner miteinander, wobei auf dem einen ein Client- und auf dem anderen der Serverprozeß laufen. Der Clientprozeß ist meistens mit einem Benutzerinterface verbunden (ein Programm, das es einem Benutzer erlaubt, komfortabel Eingaben zu machen und Ausgaben des Anwendungsprogramms zu lesen). Der Client interpretiert die Eingaben des Anwenders und führt die Anweisung entweder selbst aus oder setzt sie in Anweisungen um und schickt sie als Auftrag dem Server. Von diesem erhält er dann die Ergebnisse des Auftrags zurück (oder nur eine Meldung über die erfolgreiche oder fehlerhafte Ausführung). In der Regel läuft der Client auf dem lokalen Arbeitsplatzrechner und der Server auf einem speziellen Serversystem im Netz. Dieser Server kann dabei weit entfernt sein, bei großen Systemen jedoch auch im gleichen lokalen Netz oder sogar auf dem gleichen Rechner wie der Client arbeiten. Auf einem Rechner können mehrere Server-Programme laufen - ein Rechner kann damit mehrere Server-Dienste zur Verfügung stellen. Wenn wir von Servern reden, sollten wir deshalb unterscheiden, ob wir von einem Server-Rechner reden oder von einem Server-Dienst bzw. dem entsprechenden Server-Programm. Der Client-Prozeß wird in der Regel auch erst bei Bedarf gestartet

## INTERNET - Möglichkeiten und Dienste

und versucht dann, Kontakt mit dem Serverprozeß aufzunehmen. Dies setzt natürlich voraus, daß der Server schon 'wartet', d. h. ständig an einem System (in der Regel im Hintergrund) speicherresident läuft. Der Server verhält sich also eher passiv und wartet auf die Anfragen eines Clients. Typischerweise kann ein Server mehrere Client-Prozesse parallel bedienen.



Der Server (bzw. das Server-Programm) stellt einen Dienst zur Verfügung, der vom Client angefordert werden kann. So gibt es z. B. spezielle Server(-programme) für den Datenaustausch über FFP, zum Abruf von WWW-Dokumenten, oder Mail-Server, welche vom Mail-Client abgesendete Post entgegennehmen und weiterleiten und ankommende Post annehmen und ablegen, bis man sie mit dem Mail-Client abrufen kann. Client und Server unterhalten sich dabei in einer speziellen Sprache - dem entsprechenden Dienstprotokoll. So gibt es ein Protokoll zwischen dem Mail-Server und dem Mail-Client (z.B. SMTP oder POP3), eines für den Dateiaustausch zwischen FTP-Client und FFP-Server, ein weiteres für WWW u.s.w. Manche Server bedienen sich zur Ausführung von Aufträgen wieder weiterer Server: Der Name-Server beispielsweise setzt die textuelle Internet-Adresse in eine numerische Adresse um.

### Ports - Eingänge für Server

Unterschiedliche Serverprogramme bzw. Serverdienste werden innerhalb eines Rechners durch unterschiedliche Ports angesprochen, wobei ein Port eine Art logischer Kommunikationseingang im Rechner bzw. Betriebssystem ist. Den verschiedenen Servern (bzw. Diensten) sind im Standardfall feste Portnummern zugeordnet. Welcher Port für welchen Dienst verwendet wird, braucht uns als Endbenutzer jedoch in der Regel nicht kümmern. Der Client sollte dies wissen. Nur in Ausnahmefällen, wenn Sie eine besondere Server-Variante oder einen anderen Port benutzen möchten, geben Sie im Client den vom Standard abweichenden Port an.

## 1.5 Dokumentation

Alle Protokolle und Vereinbarungen über das Internet sind in Dokumenten festgehalten. Ganz zu Anfang waren diese Dokumente als Diskussionsgrundlagen für einen weiten Kreis von Teilnehmern gedacht, weshalb sie den Namen 'Request for Comment', kurz RFC, erhielten. Es stellte sich jedoch heraus, daß der Kreis der Diskutierenden relativ klein war und daher auf das RFC-Dokument kein eigenes Standard-Dokument folgen mußte. Die Dokumente sind durchnummeriert und im Netz frei erhältlich (z. B. auf dem Rechner ftp.leo.org), können aber auch auf CD-ROM erworben werden. Ein RFC wird auch nicht ungültig, sondern bei Änderungen im Protokoll durch ein Nachfolgedokument ('Son of RFC xxx') ergänzt oder ersetzt. Die RFCs enthalten nicht nur technische Dokumente, sondern auch für den technischen Laien geeignete Bedienungsanleitungen. Wer sich mit den RFCs zu gebräuchlichen Diensten beschäftigt, wird feststellen, daß viele Protokolle sehr einfach gehalten sind und daher die Implementierung auf verschiedenen Rechnern schnell möglich ist. Die RFC werden vom InterNIC verwaltet.

## Status eines RFC

Durch die wachsende Anzahl TCP/IP-Standards drängte sich ein Standardisierungsprozess auf. Ein RFC durchläuft diesen Prozess und kann dabei folgende Zustände erreichen:

- **Initial:** Das Protokoll wurde zur Überprüfung eingereicht.
- **Proposed Standard:** Das Protokoll wurde als Standard vorgeschlagen.
- **Draft Standard:** Das Protokoll hat eine erste Überprüfung überstanden und mindestens zwei voneinander unabhängige Implementationen wurden realisiert. Es muss jedoch noch mit Veränderungen des Protokolls gerechnet werden.
- **Standard:** Das Protokoll wurde überprüft und als gültiger Standard anerkannt. Es gehört zum offiziellen Teil der TCP/IP-Protokollfamilie.
- **Experimental:** Das Protokoll wurde nicht für Standardisierungszwecke überprüft, wird aber in Tests und Versuchen eingesetzt.
- **Historic:** Das Protokoll gilt als veraltet und wird derzeit nicht mehr benutzt.

## Bedeutung eines RFC

Das IAB legt für jedes Protokoll eine Bedeutung fest. Diese Bedeutung definiert, unter welchen Bedingungen das Protokoll eingesetzt werden soll.

- **Required:** Sämtliche Hosts und Router, die TCP/IP benutzen, müssen dieses Protokoll unterstützen.
- **Recommended:** Es wird empfohlen, dass sämtliche Hosts und Router dieses Protokoll unterstützen.
- **Elective:** Es ist freigestellt, dieses Protokoll auf Hosts und Router zu implementieren.
- **Limited Use:** Dieses Protokoll ist für die Benutzung durch Testgruppen gedacht und nicht für den allgemeinen Gebrauch freigegeben.
- **Not Recommended:** Die Benutzung dieses Protokolls ist nicht erwünscht. Veraltete Protokolle erhalten diese Bedeutung.

Zusammenhang zwischen Status und Bedeutung

	Required	Recommended	Elective	Limited Use	Not Recommended
Standard	o	*	*		
Draft	o	o	*		
Proposal		o	*	o	o
Experimental			o	*	o
Historic				o	*

Legende: \* bevorzugter Zustand, o möglicher Zustand

Jeder kann RFCs schreiben. Um ein Dokument als RFC zu publizieren, muss es allerdings beim "RFC-Chefredaktor" eingereicht werden. Dieser "RFC-Redakteur" heisst im Internet *RFC-Editor* und ist unter <http://www.rfc-editor.org> erreichbar. Der *RFC-Editor* ist Mitglied des IAB.

## 1.6 Der Internet-Wurm

Mit dem Internet-Wurm ("Morris-Wurm") vorlor das Netz seine Unschuld. Am Nachmittag des 2. Novembers 1988 wurde dieser von seinem Programmierer, Robert Tappan Morris, freigesetzt. Zu dieser Zeit war Morris noch Student an der Universität von Cornell. In der Folge wurden ungefähr 6.000 Computer weltweit lahmgelegt. Entdeckt wurde das Programm nur durch einen

Programmierfehler.

Irgendwann entdeckte Morris im Berkley UNIX zwei Fehler, die nicht autorisierten Zugriff auf Maschinen im gesamten Internet ermöglichten. Damals umfaßte das Netz schon zirka 60.000 Computer. Wieso Morris den Wurm geschrieben hat, ist nicht klar. Auch wurde nicht untersucht, ob es sich nur einen verunglückten Test oder böse Absicht handelte.

Technisch betrachtet bestand der Internet-Wurm aus zwei Programmen:

- Der Bootstrap  
Dieses kleine C-Programm wurde auf dem angegriffenen System compiliert und dann ausgeführt. Es stellte eine Verbindung zu dem Rechner her, von dem es kam und lud von dort das eigentliche Wurm-Programm und startete es.
- Der Wurm  
Dieser tarnte sich dann als Shell, um nicht erkannt zu werden. Er untersuchte die Routing-Tabelle des Rechners, um herauszufinden, mit welchen anderen Computern dieser verbunden war, um dorthin das Bootstrap-Programm zu verbreiten.

Um den nicht autorisierten Zugriff zu neuen Computern zu bekommen, um dort dann das Bootstrap-Programm zu compilieren und zu starten, hatte der Internet-Wurm vier Methoden:

- fingerd  
Eine bestimmten Funktion der Standard-C-Bibliothek, welche die Länge der Parameter nicht überprüft, wurde im FINGER-Daemon verwendet. Beim Aufruf des Daemon auf einem Remote-Rechner durch einen aktiven Wurm-Prozeß wurde eine Zeichenkette als Parameter übergeben, deren Länge den zur Verfügung stehenden Puffer-Bereich überstieg. Dadurch wurden Teile des Daemon-Prozesses im Hauptspeicher überschrieben, darunter auch die Rücksprungadresse der gerade ausgeführten Funktion. Die neue Rücksprungadresse zeigte auf einen Teil des überschriebenen Speichers, in dem jetzt eine Shell mit den Rechten des Daemon aufgerufen wurde. Mit dieser Shell wurde dann eine Kopie der für den Start des Wurms auf diesem Rechner benötigten Dateien übertragen und ausgeführt.
- sendmail  
Auch dieser Fehler war bereits bekannt; nur ein Teil der Systeme wies ihn noch auf. Die betroffenen Versionen dieses Mail-Daemon waren mit der Debug-Option kompiliert worden. Dabei wurde eine durch den Entwickler eingebaute Falltür aktiviert, die auf dem Remote-System die Interpretation einer über Electronic Mail empfangenen Nachricht als Befehl erlaubte. So konnte ein Wurm-Prozeß auf einem Remote-Rechner eine Shell starten.
- rsh  
Eine wichtige Eigenschaft vieler UNIX-Systeme ist das Konzept des "distributed trust", das mit den sogenannten 'r'-Protokollen der BSD-Implementation eingeführt wurde. Inzwischen werden diese Protokolle auch in anderen UNIX-Derivaten eingesetzt. Mit ihrer Hilfe ist es möglich, auf anderen Rechnern bestimmte Befehle oder eine Remote-Shell aufzurufen, wenn der lokale Rechner dort als vertrauenswürdig eingestuft ist. Diese Einstufung erfolgt durch den Eintrag der Rechnernamen in eine spezielle Datei. Da in der Regel eine solche Einstufung auf Gegenseitigkeit beruht, versuchte der Wurm-Prozeß, auf den in der lokalen Datei angegebenen Rechnern eine Remote-Shell zu starten.
- Paßwörter knacken  
Durch die Möglichkeit, auf die gespeicherten Benutzer- Identifikationen und die zugehörigen, verschlüsselten Paßwörtern zuzugreifen, konnte der Wurm-Prozeß einen Brute-Force-Angriff auf einen Account durchführen. Gelang es, durch Ausprobieren ein Paßworts herauszubekommen, wurde mit damit versucht, auf einem anderen Rechner des Netzwerks eine Shell zu starten. Dies gelang, wenn der jeweilige Benutzer auf diesem Rechner das gleiche Paßwort verwendete. Da sein Vater als Sicherheitsexperte bei der *National Security Agency* 10 Jahre zuvor einen Bericht über genau dieses Thema geschrieben hatte, brauchte

## INTERNET - Möglichkeiten und Dienste

Morris nicht viel Erfahrung in diesem Bereich.

Die Entdeckung des Wurm beruht auf einem kleinen Denkfehler von Morris. Der Wurm hat so gearbeitet, daß er nur Computer angriff, die nicht schon vom Wurm befallen waren. In einem von 15 Fällen sollte trotzdem ein Wurm gestartet werden, um sicherzustellen, daß der Wurm nicht stirbt (z. B. bei Vortäuschung eines Wurmbefalls). Leider wurde in 14 von 15 Fällen der Wurm repliziert, so daß einige Computer so stark an Leistung verloren, daß die Administratoren aufmerksam wurden.

Gefaßt wurde Morris durch einen Versprecher einer seiner Freunde während eines Interviews. Dieser erzählt dem Reporter von der *New York Times*, daß der Wurm nur ein Unfall war und es dem Autor leid tut. Dabei rutscht ihm der Benutzername heraus, so daß es nicht mehr schwer war, den wirklichen Namen zu ermitteln. Das Gericht verurteilte Morris zu \$ 10000 Strafe, 3 Jahren Haft und 400 Stunden gemeinnützige Arbeit. Zusätzlich entstanden \$ 150.000 Gerichtskosten.

Nach der Verurteilung von Morris gab es eine große Kontroverse. Teils wurde die Meinung vertreten, er sei intelligenter Student, der nur etwas gespielt habe. Von anderen wurde er für einen Kriminellen gehalten, der ins Gefängnis müsse.

Als unmittelbare Folge wurde im Dezember 1988 ein sogenanntes "Computer Emergency Response Team" (CERT) ins Leben gerufen. Heute kontrolliert das CERT Coordination Center die Tätigkeit verschiedener CERTs. Es gibt eine Telefon-Hotline und verschiedene Publikationsorgane, die auf Sicherheitslücken hinweisen und den Anwendern Hilfestellung geben. Nach dem Vorbild der CERTs wurden seitdem weltweit ähnliche Gruppen aufgebaut.

### 1.7 Zukunftstendenzen (Stand 2002)

Quelle: Beck/Glotz/Vogelsang: Die Zukunft des Internet, Konstanz, ISBN 3-89669-287-9

- Der Prozess der Medienintegration sichert bis zum Jahr 2010 etwa 25 bis 40 Prozent der privaten Haushalte in den entwickelten Industriestaaten einen universellen und regelmäßig genutzten Zugang zu digitalen Medien und Kommunikationsdiensten.
- Die Nutzung der Computernetze wird mit Hilfe unterschiedlicher Endgeräte erfolgen - die "universelle Kommunikationsmaschine" wird also allenfalls eine digitale, vielleicht TCP/IP-basierte Infrastruktur sein, nicht jedoch die Gestalt eines einheitlichen Interface annehmen.
- Die bekannten Modi der Mediennutzung (Unterhaltung, Information, Kommunikation) werden in ihren Grundzügen erhalten bleiben; auf der Angebotsseite kommt es zu einer Kommerzialisierung und Segmentierung. Die Trennung von redaktionellem Inhalt, PR und Werbung wird weiter erodieren, zumal auch Markenartikler und andere Unternehmen selbst zu Anbietern von Medieninhalten werden.
- Die direkte Kommunikation (Face-to-face) wird ihre sehr hohe soziale Bedeutung behalten, E-Mail wird Teile des Telefon- und Briefverkehrs substituieren. Im übrigen werden computervermittelte Kommunikationsformen als zusätzliche Chance für die Erweiterung des persönlichen sozialen Netzwerks und die Teilhabe in virtuellen Gemeinschaften global genutzt.
- Ausschlaggebend für die Wahl eines bestimmten Mediums bzw. eines Kommunikationsmodus bleibt - trotz erweiterter Wahlmöglichkeiten - der Beziehungsaspekt: Entscheidend ist, mit wem (Partner, Familie, Freunde, Bekannte oder Fremde) man kommunizieren will, und weniger, welcher Anlass oder Zweck (Task orientation) damit verfolgt wird.
- Bildung, Einkommen und Lebensstil (z.B. großstädtische, erwerbstätige Singles) bleiben auch in den nächsten 10 bis 15 Jahren prägende Kriterien für die regelmäßige Online-Nutzung. Die "Digital divide" könnte also zu einem nachhaltigen Problem unserer Gesellschaft werden.
- Im Bildungswesen trägt der Prozess der Medienintegration zur Entwicklung eines spezialisierten Bildungsnetzes bei, ohne dass es mittelfristig zu strukturellen Umwälzungen

## INTERNET - Möglichkeiten und Dienste

im Institutionen-Gefüge der Allgemeinbildung (Schulen und Hochschulen) kommen wird. Die virtuelle Universität wird im nächsten Jahrzehnt nicht zum Regelfall.



- Wachsende Wissensklüfte, soziale Ungleichheit und divergierende Medienkompetenzen begleiten zumindest mittelfristig den Prozess der Medienintegration. Dies gilt nicht nur im globalen Maßstab, sondern auch für entwickelte Industrie- bzw. "Informationsgesellschaften".
- Im wissenschaftlichen Publikations- und Bibliothekswesen ermöglicht die Medienintegration einschneidende Veränderungen: Bibliotheken werden ihr Dienstleistungsangebot erweitern und elektronische Texte (preprints) werden den wissenschaftlichen Diskurs sowie den Wissenstransfer verändern. Prognostiziert wir u.a., dass Wissenschaftler noch unabgeschlossene Publikationen im Netz zur Diskussion stellen und der Scientific community die Möglichkeit geben, an diesen Texten weiter zu schreiben. Ein solches "Ende des Autors" könnte weitreichende Folgen auf das gesamte Reputationswesen der Wissenschaft zeitigen.
- Electronic-Commerce ist das Epizentrum der Entwicklungen zur "Informationsgesellschaft", wobei einzelne Branchen sehr unterschiedlich betroffen sind. Marketing und Vertrieb sowie die gesamte Wertschöpfungskette unterliegen einem strukturellen Wandel. Vor allem "immaterielle" Güter wie Software und Musik, aber auch Bücher und EDV-Hardware werden in deutlich höherem Maße online verkauft als beispielsweise Lebensmittel, Kleidung, Möbel oder Autos.
- Im Business-to-consumer-Sektor erweisen sich E-Banking und E-Booking als Vorreiter; Das Filialgeschäft der Banken und die Reisebüros werden hiervon in sehr hohem Maße betroffen sein. Zu den Verlierern werden außerdem die Videotheken gehören, die sich gegen digitale Video-on-demand- Angebote nicht mehr lange werden behaupten können.
- Kurz- und mittelfristig sind leicht negative Beschäftigungseffekte zu erwarten (Netto-Arbeitsplatz-Bilanz), zunächst vor allem in den Industriestaaten.
- Alternierende Telearbeit wird primär von geringer Qualifizierten im Dienstleistungssektor geleistet; die Erwerbsverhältnisse werden sich durch- und tiefgehend wandeln. Feste, arbeitsrechtliche besonders geschützte Beschäftigungsverhältnisse werden mehr und mehr projektbezogenen Kooperationen weichen. Erwerbstätige werden als "Selbstbeschäftigter" vorrübergehender "Teil" oder Partner virtueller Unternehmen.

Auch von mir noch ein paar Bemerkungen (2008):

- Stärkstes Hemmnis waren die Kosten für Hardware und Zugang - durch preiswerte PCs und DSL-Flatrate heute kein Problem mehr. An Stelle von Modem und ISDN sind schnelle DSL-Verbindungen getreten. Teilweise dienen auch Funk-Netze (WLAN, WiMAX) als Zugang und u. a. auch öffentliche WLAN-Zugänge.
- E-Commerce: Der 2002 beklagte Mangel an Benutzerfreundlichkeit, zu hohen Vertriebskosten und antiquierten Zahlungsmodalitäten ist auch heute noch vielfach anzutreffen. Auch das Internet-Business hat sich weiterentwickelt, obwohl auch Anbieter wie Amazon oder EBay bisher mal "gerade so" in den schwarzen Zahlen sind. Im B2B-Bereich ist es dagegen jetzt erfolgreich.
- Das Buch und die Zeitschrift werden nicht sterben - jedoch einzelne Titel oder Gattungen, so erscheint der Brockhaus seit 2008 nur noch online (Was stellen jetzt die Neureichen bloss ins Regal?).
- Persönliche Kontakte werden immer noch wichtiger als virtuelle sein
- 2002 schrieb ich: "WAP ist schon fast tot und UMTS wird sich zum Flop entwickeln. Einzige Rettung für UMTS: Migration von GSM nach UMTS". Jetzt kommt zaghaft die *kostengünstige Internet-Anbindung über UMTS*.
- Bandbreiten werden ausgebaut - Folge: noch bunter, noch zappeliger!
- Neue Applikationen werden entstehen (Beispiele: Napster, Gnutella, P2P) Was vielfach nicht begriffen wird, ist die Tatsache, dass Jedermann jederzeit ein neues Protokoll "erfinden" kann und damit auch völlig neue Anwendungen entstehen können.
- Es wird **keine** Konvergenz der Medien geben (hat schon bei Heimcomputern, Videospielen und BTX nicht geklappt)

## INTERNET - Möglichkeiten und Dienste

- Neu hinzugekommen ist auch die Erkenntnis, dass die bisherigen Protokolle nicht immer die für eine neuartige Anwendung nötigen Eigenschaften besitzen. Speziell beim WWW merkt man das an den Webseiten, die durch Java, JavaScript bzw. Ajax, PHP, usw. mühsam "aufgemotzt" werden müssen. In diese Richtung geht auch das, was Tim O'Reilly mit "WEB 2.0" bezeichnet hat ([What is Web 2.0?](#) bzw. [Web 2.0-Links](#))

Es sind einige Dienste verschwunden bzw. vom World Wide Web "aufgesogen" worden (inzwischen wird ja oft "Internet" und "WWW" als Synonym betrachtet), z. B. Archie, Gopher, Wais. Im Grunde gibt es nur noch einen Suchdienst: Google.  [Zum Inhaltsverzeichnis](#)  [Zum nächsten Abschnitt](#)

---

Copyright © Prof. Jürgen Plate, Fachhochschule München



## INTERNET - Möglichkeiten und Dienste

*Prof. Jürgen Plate*

---

## 2 Internet-Dienste im Überblick

*"The Information Superhighway is a misnomer.  
First, there's no highway - there are no roadmaps,  
guides, rules. And second, it ain't super."  
David Martin.*

Die einzelnen Dienste, die man heute im Internet in Anspruch nehmen kann, haben sich nach und nach entwickelt. Zu Beginn wurde die Basis des Internets von den drei Diensten elektronische Post, Telnet und FTP gebildet. Später kamen dann Informationsdienste wie News, Archie, Gopher und WAIS hinzu. Der jüngste Dienst ist WWW, der nahezu alle anderen Dienste integrieren kann. Deshalb fange ich mit dem wichtigsten Basisdienst, der elektronischen Post, an und schließe mit WWW den Überblick.

### 2.1 Die elektronische Post

Ein Beispiel: Sie haben gerade eine tolle Werbung für Ihr neues Gerät entworfen und möchten sie von Ihrem Geschäftsfreund in Amerika überprüfen lassen. Sie schicken ihm rasch eine elektronische Post (Electronic Mail, E-Mail) über das Internet. Dieser holt sich das Dokument auf seinen Bildschirm, bringt ein paar Korrekturen an und schickt Ihnen das Dokument zurück. Beide bezahlen für diese Transatlantik-Operation nicht mehr als ein paar Pfennige - wesentlich weniger als für ein Telefongespräch.

*E-Mail:* Inzwischen ist es schick, eine E-Mail-Adresse auf der Visitenkarte zu haben. Auch in Veröffentlichungen in Zeitungen und Zeitschriften finden sich Mail-Adressen der Autoren und Herausgeber als Möglichkeit der Kontaktaufnahme. Der 'Klammeraffe' wird in Namen von Produkten, Firmen und Zeitschriften als Ersatz für das 'a' verwendet (sprachlich ein Paradox, denn das ASCII-Zeichen '@' wird 'at' ausgesprochen).

Bei E-Mail (auch 'Email', 'e-mail' oder schlicht nur 'Mail' genannt) handelt es sich um einen schnellen, bequemen Weg, Nachrichten bzw. Dokumente zwischen Rechnersystemen mit dem gewünschten Partner auszutauschen. Obwohl E-Mail der einfachste (und auch wohl älteste) netzübergreifende Dienst ist, will ich ihn etwas ausführlicher behandeln. Die anderen Dienste sind dann um so leichter zu verstehen.

Computer, die mit einem Multiuserbetriebssystem ausgestattet sind, also Systeme, bei denen mehrere Anwender (quasi-)gleichzeitig arbeiten können, besitzen nahezu alle die Möglichkeit, daß sich diese Anwender auch untereinander verständigen können. Das geschieht mittels eines kleinen Programms, das es ermöglicht, Nachrichten zu schreiben und diese dann an einen gewünschten Empfänger zu schicken. Der Adressat erhält dann beim nächsten Login den Hinweis auf neu eingegangene Post. Je nach Verbindung zu anderen Rechnern wird die Nachricht direkt zum Empfänger geschickt oder über einige Zwischenstationen geleitet (hier zeigt sie die Analogie zur althergebrachten Post). Für diese Art des Versendens von Mitteilungen hat sich sehr schnell der englische Begriff 'Mail' (auf deutsch 'Post') eingebürgert. Und da es sich nicht um eine Post im üblichen Sinne handelt, also auf Papier geschrieben und im Umschlag überreicht, bezeichnet man das Ganze als 'Electronic Mail' oder kurz 'E-Mail'. Auch im Deutschen haben sich die englischen Begriffe 'Mail' und 'E-Mail' etabliert. Wird ein Computer an ein Netz angeschlossen, kann die E-Mail nicht nur an Benutzer auf dem lokalen System, sondern auch an Benutzer jedes Rechners im Netz versendet werden. Ist das Netz seinerseits an das Internet angeschlossen, kann die E-Mail prinzipiell an jeden Benutzer eines Rechners im Internet versendet werden.

Die E-Mail gewann in den letzten Jahren spürbar an Bedeutung, sowohl in der Wirtschaft als auch in der Technik, da es sich gezeigt hat, daß diese Art der Kommunikation die schnellste ist, die es gibt. Es ist eine Tatsache, daß die Erfolgsquote bei der E-Mail sogar noch höher liegt als beim Telefon.

## INTERNET - Möglichkeiten und Dienste

Mit Erfolgsquote ist gemeint, daß man die Nachricht nach dem Absenden vergessen kann; man muß nicht warten, bis man den Empfänger eventuell erst nach mehreren Versuchen erreicht (z. B. mehrmals Anrufen oder warten, bis das Faxgerät beim Empfänger frei ist). Heutzutage ist E-Mail nicht nur mehr auf einem Mehrbenutzer-Computersystem üblich. Man verteilt vielmehr die Post an andere Rechner, so daß überregionale Kommunikation per E-Mail abgewickelt werden kann.

### **Weg eines normalen Briefes**

Electronic Mail ist in vielen Bereichen analog zur normalen sogenannten gelben Post aufgebaut (von den Fans der Electronic Mail auch 'snail mail' = Schneckenpost genannt). Deshalb soll zuerst noch einmal der Lebensweg eines (normalen) Briefes aufgezeigt werden. Ein normaler Brief, z. B. ein Geschäftsbrief, besteht aus zwei Teilen. Zuerst kommt der Briefkopf mit den Adressen von Empfänger und Absender, dem Datum, einer Betreffzeile usw. Darauf folgt der eigentliche Inhalt des Briefes und eventuell ein paar Anlagen. Nachdem der Brief geschrieben wurde, wird er in einen Umschlag gesteckt und dieser Umschlag mit der Adresse des Empfängers und des Absenders versehen. Zusätzlich kann er spezielle Versand-Vermerke bekommen.

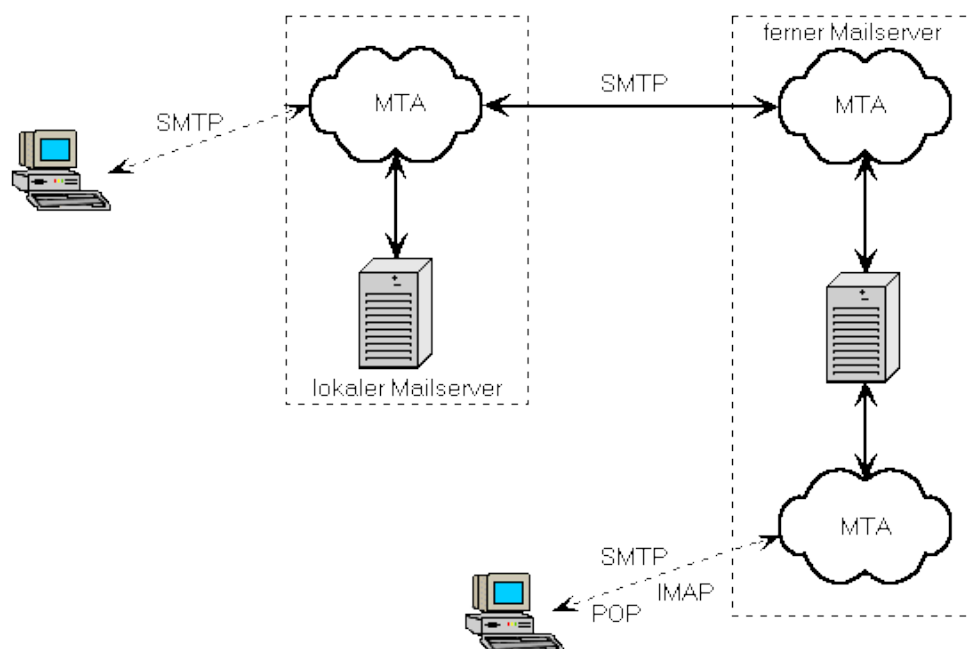
Anschließend wird der Brief in einen gelben Briefkasten der Deutschen Bundespost geworfen. Der Briefkasten wird geleert und die Briefe werden zu einem Postamt gebracht. Dort werden sie sortiert, und es wird entschieden, wohin der Brief als nächstes gebracht werden soll. Es kann sein, daß der Brief im gleichen Postamt bleibt, oder aber er wird von einem Postamt zum anderen weitergegeben, bis er bei dem Postamt landet, in dessen Zustellbezirk der Empfänger wohnt. Ein Postbote bekommt den Brief und liefert diesen in den Briefkasten des Empfängers aus bzw. übergibt ihn eingehändig an den Empfänger, wenn der Brief ein Einschreiben ist. Oder aber der Brief kommt in ein Postfach an diesem Postamt. Der Umschlag wird entfernt, der Brief wird gelesen, dann weggeworfen oder in einer Ablage aufbewahrt.

### **Weg eines elektronischen Briefes**

Auf einem Computer wird mit einem Editor der Inhalt des Briefes in eine Datei geschrieben und mit Hilfe eines Mail- Programms mit Umschlag und Empfängeradresse versehen und in die Ausgangs-Mailbox gelegt. Den ersten Teil des Briefes nennt man 'Header', den Inhalt und die Anlagen 'Body Parts'. Der Umschlag heißt auf englisch 'Envelope' (letzterer hat hauptsächlich etwas mit dem Übertragungsprotokoll zu tun, der Normalanwender bekommt ihn nicht zu Gesicht). D. h. eine Mail, die an das Mail- System übergeben wird, besteht aus dem Envelope, dem Header und einem oder mehreren Body Parts. Die Postboten und Postämter nennt man 'Message Transfer Agents' (MTA), die zusammen das 'Message Transfer System' (MTS) bilden. Dieses MTS sorgt dafür, daß eine Mail von einem Rechner zum anderen gelangt.

Beim Ziel-MTA angelangt, wird die Mail in die Eingangs- Mailbox des Empfängers gelegt. Der Empfänger kann sich dann mit Hilfe eines Mail-Programms seine Mail aus dem Postfach in seine Eingangs-Mailbox holen und lesen. Wenn er sie danach nicht wegwirft, wird er sie in eine Ablage kopieren, die man 'Folder' nennt. Die Benutzeroberfläche zum Erstellen einer Mail, die Eingangs- und Ausgangs-Mail-Boxen, die Folder und eine eindeutige Mailadresse zusammen nennt man den 'Mail User Agent' (MUA) oder 'Mailer'.

## INTERNET - Möglichkeiten und Dienste



Je nach verwendetem Mail-System gibt es meist noch weitere Funktionen, z. B. das Weiterleiten von Nachrichten (ggf. mit Kommentar), Versenden von Nachrichten an mehrere Empfänger, Benachrichtigung des Versenders einer Nachricht, daß Mail beim Empfänger angekommen und gelesen wurde. Übrigens, wenn Sie nur den Rechner, aber nicht die genaue Benutzerkennung wissen, dann schreiben Sie versuchsweise an den 'postmaster' des Systems. Der 'postmaster' ist die Mail-Adresse, bei der alle Fehlermeldungen, aber auch Anfragen von außen, z. B. nach Benutzerkennungen, anlaufen. Dahinter versteckt sich normalerweise der Systemverwalter. Briefe, die an einen anderen Computer gehen, werden in der Regel sofort abgeschickt, so daß sie der Empfänger im Internet in kurzer Zeit erhält. Briefe, die innerhalb eines Systems verschickt werden, erreichen ihren Empfänger ein paar Sekunden nach dem Abschicken.

Rechner mit direkter TCP/IP-Verbindung tauschen ihre E-Mail direkt aus. Das Protokoll heißt SMTP (Simple Mail Transfer Protocol). Hier wird die E-Mail dem Zielrechner direkt zugestellt, mehr dazu im Kapitel 4. Die E-Mail kann nicht nur über das Netz transportiert werden, sondern auch z. B. über eine Modemverbindung über die normale Telefonleitung, weshalb wesentlich mehr Rechner via E-Mail erreichbar sind als im Internet existieren. Auch die Benutzer von Mailboxnetzen wie CompuServe, AOL oder T-Online sind per E-Mail erreichbar. Außerdem gibt es auch Erweiterungen der Mail-Software, die das Nachsenden der elektronischen Post an jeden Ort der Welt oder das Bereithalten zur Abholung ermöglichen. Es gibt sogar automatische Antwortprogramme (z. B. für Infodienste).

### Was ist MIME?

Der erste Mail-RFC 822 legte in erster Linie den Standard für Kopfzeilen in der elektronischen Post fest. Dort wurde unterstellt, beim Inhalt des Briefes handele es sich um reinen ASCII-Text. Wer Dateien versenden wollte, die Zeichen enthielten, welche nicht unter den 128 Zeichen des ASCII-Alphabets vorkamen, mußte die Datei so codieren, daß sie nur noch aus ASCII-Zeichen bestand.

MIME (Multipurpose Internet Mail Extensions) fügt diesem Standard vier weitere Felder hinzu, die genauer den Inhalt des Briefes spezifizieren. Aus diesen Feldern kann das Post-Programm, so es diese berücksichtigt, entnehmen, welche anderen Programme aufzurufen sind, um z. B. ein Bild darzustellen. Das heißt nicht, daß die Daten im Brief nicht codiert würden, aber ein MIME-konformes Post-Programm bietet die Möglichkeit, alle Codierungsvorgänge zu automatisieren.

## INTERNET - Möglichkeiten und Dienste

Das erste Feld, welches der MIME-Standard definiert, heißt MIME-Version:. Bislang gibt es nur die Version 1.0, so daß der Eintrag 1.0 dem Standard genügt. Mit der Verwendung dieses Feldes wird dem Post-Programm signalisiert, daß der Inhalt des Briefes mit dem MIME-Standard konform geht.

Kannnte der RFC 822 zwei Teile eines Briefes, nämlich den Kopf und den Text, so können Briefe im MIME-Format aus mehreren Teilen bestehen. Die Zeile `MIME-Version: 1.0` muß nur einmal im Kopf des Briefes auftauchen. Die anderen Felder, welche der MIME-Standard definiert, können öfter verwendet werden. Sie beschreiben dann jeweils die Einzelteile, aus denen der Brief besteht. Ein Beispiel:

```
...
MIME-Version: 1.0
Content-Type: MULTIPART/MIXED; BOUNDARY="8323328-2120168431-
824156555=:325"

--8323328-2120168431-824156555=:325
Content-Type: TEXT/PLAIN; charset=US-ASCII

Textnachricht....

--8323328-2120168431-824156555=:325
Content-Type: IMAGE/JPEG; name="teddy.jpg"
Content-Transfer-Encoding: BASE64
Content-ID: <Pine.LNX.3.91.960212212235.325B@localhost>
Content-Description:
/9j/4AAQSkZJRgABAQAAQABAAD//gBqICBjBvbnRlZCBmcm9tIE1JRkYg
aWlhZ2U6IFh0ZWRkeQoKQ1JFQVRPUjogWFYgVmVyc2lvbiAzLjAwICBSZXY6
[... ]
se78SaxeW7Qz3zeW33tqqu7/AHtv3qyaKmOGox96MSeSIUUUVuUFFFFFFABRRR
RZAFFFFABRRRTAKKKKACiigAooooA//2Q==
--8323328-2120168431-824156555=:325--
```

Mit dem Feld "Content-Type:" wird der Inhalt eines Briefes beschrieben. Im Kopf des Briefes legt das Feld "Content-Type:" den Aufbau des ganzen Briefs fest. Das Stichwort `Multipart` signalisiert, daß der Brief aus mehreren Teilen besteht. Der Untertyp von "Multipart" `Mixed` liefert den Hinweis, daß der Brief aus heterogenen Teilen besteht. Der erste Teil dieses Beispiels besteht denn auch aus Klartext, und der zweite Teil enthält ein Bild. Die einzelnen Teile des Briefes werden durch eine Zahlenkombination eingegrenzt, die im Kopf des Briefes im Feld "Boundary" festgelegt wurde. Diese Grenze (Boundary) ist nichts weiter als eine eindeutig identifizierbare Zeichenfolge, anhand derer die einzelnen Teile einer E-Mail unterschieden werden. Ein MIME-konformes Post-Programm sollte anhand dieser Informationen jeden einzelnen Teil adäquat darstellen können. Im Feld "Content-Type:" können sieben verschiedene Typen festgelegt werden, die jeweils bestimmte Untertypen zur genaueren Beschreibung des Inhalts umfassen:

- text: plain, enriched, html
- multipart: mixed, alternative, parallel, digest
- message: rfc822, partial
- image: jpeg, gif
- audio: basic
- video: mpeg
- application: octet-stream, PostScript, active

Die Typen "image", "audio", "video" sprechen für sich selbst. Der Typ "message" sollte dann verwendet werden, wenn der Brief einen anderen Brief enthält. (z. B. einen weitergeleiteten Brief). Der Typ "application" ist für die Beschreibung ausführbarer Programme gedacht.

Dem Typ "text" kann noch der Parameter "charset:" beigefügt werden. Die Vorgabe der Programme lautet in der Regel "charset: us-ascii". Anstelle von "us-ascii" kann hier auch "iso-8859-1" eingetragen

## INTERNET - Möglichkeiten und Dienste

werden. Inzwischen werden auch vielfach E-Mails, markiert durch "text/html", wie HTML-Seiten codiert (beim Netscape-Browser ist sogar Klartext und HTML-Darstellung voreingestellt, man bekommt den Brief also doppelt).

Über kurz oder lang stößt wohl jeder Benutzer der elektronischen Post auf folgende Zeichen: =E4, =F6, =FC, =C4, =D6, =DC, =DF; im Klartext: ä, ö, ü, "A, "O, "U, ß. Für den Fall, daß der Brief Zeilen enthält, die länger als 76 Zeichen sind, erscheint ein "="-Zeichen am Ende der Zeile für den automatischen Zeilenumbruch. Verantwortlich für dieses Phänomen ist der Eintrag "quoted-printable" im Feld "Content-transfer-encoding". Mit der Vorgabe "quoted-printable" soll ein MIME-konformes Post-Programm alle Zeichen, deren Wert größer als 127 ist, hexadezimal mit einem vorangestellten Gleichheitszeichen darstellen, und es soll Zeilen, die länger als 76 Zeichen sind, umbrechen. Unter Umständen werden noch einige andere Zeichen codiert. Einige Post-Programme verwenden von vornherein "quoted-printable", obwohl eine andere Belegung des Feldes möglich ist; z. B.: "7bit", "8bit", "binary", "base64". Die ersten drei signalisieren allgemein, daß keine Codierung vorgenommen wurde. "7bit" signalisiert insbesondere, daß ein Brief reine ASCII-Zeichen enthält; "8bit", daß ein Brief über den ASCII-Zeichensatz hinausgeht, und "binary", daß es sich um 8-Bit-Zeichen handelt, wobei die Zeilenlänge über 1000 Zeichen hinausgehen kann. Ein mit "base64" codierter Teil des Briefes besteht nur noch aus Zeichen, die mit 7 Bit dargestellt werden können. Der Vorteil dieses Codierungsverfahrens besteht im Gegensatz zu anderen darin, daß diese Untermenge in vielen anderen Zeichensätzen ebenfalls enthalten ist. Damit wird eine fehlerfreiere Übermittlung erreicht, als mit anderen Verfahren.

### Base64-Codierung

In Fällen, in denen binäre Dateien (Image, Audio) codiert werden müssen, wird die Encoding-Regel "Base64" verwendet, die Bitfolgen einer byteweise organisierten Datei in ein Alphabet aus 64 Textzeichen des ASCII-Zeichensatzes übersetzt. Da nur 64 Zeichen (lesbare) dargestellt werden, bedeutet dies, daß lediglich sechs Bit zu einem Zeichen zusammengefasst werden. Insgesamt wird die Datei in Gruppen zu 24 Bit (drei Bytes) strukturiert. Das Ergebnis für jede dieser 24-Bit-Gruppen ist eine Folge aus vier ASCII-Zeichen. Die Übersetzung erfolgt seriell nach der Regel einer Code-Tabelle: Zunächst werden die ersten sechs Bit in ein ASCII-Zeichen übersetzt. Das bedeutet, daß vom ersten byte noch zwei Bit uncodiert sind. Diese beiden Bit des ersten bytes sowie die ersten vier Bit des folgenden bytes werden in ein Zeichen übersetzt und so weiter. Das Prinzip ist denkbar einfach, allerdings hat dieses Verfahren, das mittlerweile etabliert ist, einen kleinen Schönheitsfehler, denn die Nachrichten werden in codierter Form bedeutend länger.

Wert	Code	Wert	Code	Wert	Code	Wert	Code
0	A	17	R	34	i	51	z
1	B	18	S	35	j	52	0
2	C	19	T	36	k	53	1
3	D	20	U	37	l	54	2
4	E	21	V	38	m	55	3
5	F	22	W	39	n	56	4
6	G	23	X	40	o	57	5
7	H	24	Y	41	p	58	6
8	I	25	Z	42	q	59	7
9	J	26	a	43	r	60	8
10	K	27	b	44	s	61	9
11	L	28	c	45	t	62	+
12	M	29	d	46	u	63	/
13	N	30	e	47	v		

## INTERNET - Möglichkeiten und Dienste

14	O	31	f	48	w		
15	P	32	g	49	x		
16	Q	33	h	50	y		
Padding: =				Quelle: RFC 2045			

Der Begriff "Text" ist nicht damit gleichzusetzen, daß das Ergebnis der Codierung auf den ersten Blick lesbar ist. Die Buchstaben, Ziffern und die Zeichen "+", "/" und "=" dienen lediglich als Symbole für die entsprechenden Bitfolgen. Die Tabelle zeigt die Übersetzung gemäß "Base64", wobei die Angabe der Werte in den zu übersetzenden Bitfolgen (jeweils sechs Bit) in dezimaler Schreibweise erfolgt. Das Zeichen "=" hat eine besondere Bedeutung, denn es dient als Füllzeichen (Padding), wenn die Menge der zu übertragenden Zeichen aus den Quelldaten kein Vielfaches von vier darstellt. Die Übertragung dieser Zeichen erfolgt in Textzeilen, die maximal 76 Zeichen beinhalten. Alle nicht im Base64-Alphabet definierten Zeichen einschließlich Zeilenumbrüchen werden bei der Decodierung ignoriert.

### Was bei E-Mail schiefgehen kann

Natürlich können auch bei E-Mail Probleme auftreten. Schließt man allerdings aus, daß das eigene System nicht korrekt aufgesetzt ist, der POP nicht korrekt arbeitet oder der Name-Server nicht funktioniert, so verbleiben folgende häufigeren Fehlerquellen:

- Die Adresse ist falsch.  
Dabei kann entweder der Adressat selbst nicht existieren oder falsch geschrieben sein oder Sie haben einen Fehler bei der Angabe der Domain-Angabe (des Mail-Servers) gemacht. Nach einiger Zeit kommt dann die Mail mit etwa folgender Nachricht zurück:

```
From: Mail delivery Subsystem
Subject: Returned mail: Host unknown
(Name server: ns.e-technik.fh-muenchen.de: host not found)
```

oder

```
From: Mail delivery Subsystem
Subject: Returned mail: User unknown
```

überprüfen Sie nochmals die Adreßangabe. Haben Sie bei einer Mail-Adresse in einem anderen Netzwerk die Übersetzungskonventionen richtig beachtet?

- Der Mail-Server ist nicht erreichbar.  
Versuchen Sie es später nochmals. Haben Sie weiterhin Probleme, sollten Sie sich mit Ihrem Provider (telefonisch oder per FAX) in Verbindung setzen.
- Der Name-Server kann den Namen des Mail-Servers nicht auflösen.  
Auch hier sollten sie es später nochmals versuchen.
- Die Mail ist beim Empfänger verstümmelt oder kann nicht gelesen werden.  
Wahrscheinlich haben Sie eine unpassende Codierung verwendet oder der Empfänger kann nur reinen ASCII-Text im Mail-Programm anzeigen.
- Sie erhalten eine Mail mit Anhängen, können diese jedoch nicht anzeigen oder bearbeiten.  
Erkundigen Sie sich beim Absender, in welchem Format der Anhang sein soll. Hier ist Abstimmung erforderlich.
- Sie finden eine Mail in Ihrem Posteingang, die zu umfangreich ist.  
Die Mail ist so groß, daß die Übertragung gar nicht möglich ist oder zu lange dauert und damit zu teuer wird. Sie können die Mail löschen.
- Sie erhalten Mail mit einem großen, eigenartigen Textstück darin.  
Wahrscheinlich handelt es sich um mittels uuencode codierte Binärdaten im Mail-Anhang, der etwa wie folgt aussieht.

begin 600 DOKUMENT.DOC

## INTERNET - Möglichkeiten und Dienste

```
M(&=R; ] ]E;B!3>7-T96UE;B!J96108V@@875C: " !I; 2!G; &5I8VAE;B!L;VMA
M; &5N($YE='H@;V1E<B!S;V=A<B!A=68@9&5M(&=L96EC:&5N(%)E8VAN97(@
M=VEE(&1E<B!#; &EE;G0@87)B96ET96XN($%U9B!E:6YE;2!296-H;F5R(&OV
M;FYE;B!M96AR97)E(%-E<G9E<BU0<F]G<F%M;64@; &%U9F5N("T@96EN(%)E
M8VAN97(@:V%N;B!D86UI="!M96AR97)E(%-E<G9E<BU$:65N<W1E('IU<B!6
```

.....

end

Das Mailprogramm sollte mittels uuencode codierte Mail automatisch und ohne Zutun des Benutzers decodieren können. Ähnlich gelagert ist das Problem, wenn die Datei nach 'base64' codiert ist. Es handelt sich dabei um eine MIME-codierte Anlage. MIME-Mails sind typischerweise an den eingestreuten Steuerzeilen (Content-Type: application/octet-stream) und Trennzeilen (-----\_8769453AF34==\_) erkennbar.

### Was bedeutet "AW:" im Header?

Das bedeutet, daß Ihr Mailpartner Microsoft Outlook verwendet. Dort wird unter der Prämisse "Internationalisierung" alles gnadenlos in die Sprache des jeweiligen Landes übersetzt. So wird aus "Re:" für "reply" nun "AW:" für "Antwort". Dabei haben die Microsoftis aber übersehen, daß "Re:" im entsprechenden RFC-Dokument festgelegt wurde, also gar nicht übersetzt werden darf (das hat aber Microsoft noch nie gestört, in einer Windows-3.1-Version wurde sogar die Druckersprache Postscript mal eingedeutscht). Um lange "Re: AW: Re: AW: ..." -Ketten zu vermeiden, kann man Outlook auch wieder RFC-konform machen.

Gehen Sie dazu ins Menü "Extras, Optionen". Auf der Registrierkarte "E-Mail-Format" klicken Sie auf "Internationale Optionen" und aktivieren Sie "Nachrichtenkennzeichnungen in Englisch" und "Kopfzeilen von Antworten und Weiterleitungen in Englisch". Damit ist Outlook RFC-fest. Alle anderen Outlook-Funktionen und -Menüs bleiben natürlich in Deutsch. Bei Outlook Express finden Sie die Optionen unter "Extras, Optionen" und dann in der Registrierkarte "Senden" unter "Internationale Einstellungen". Nach diesen Änderungen ist Outlook nicht nur mit allen Mailprogrammen kompatibel, die sich an die Internet-Standards halten, sondern auch Sie selbst outen sich als Fachmann in Sachen E-Mail.

Wer mehr über die Header in E-Mails wissen will, findet hier ein [Mailheader-FAQ](#).

## 2.2 News - öffentliche Diskussionsforen

News ist ein weltweites elektronisches 'schwarzes Brett' zur Diskussion von Themen, zum Austausch und zur Beschaffung von Informationen und zur Verteilung von Daten. Dieses Kommunikationsmedium ist neben Mailing-Listen das am weitesten verbreitete System für den Austausch von öffentlichen Informationen. News ist nach den verschiedensten Interessengebieten hierarchisch geordnet. Dabei sind weltweit Tausende Themenbereiche (die sogenannten News-Gruppen) verfügbar, die von der Diskussion bestimmter Rechnertypen über die Bekanntmachung von Konferenzen bis hin zur Verteilung von Kochrezepten reichen. News baut auf NNTP (Network News Transfer Protocol) auf. Dazu benötigt ein Benutzer eine bestimmte Schnittstelle, den sogenannten News-Reader. Dies ist ein Programm, das Verbindung mit einem News-Server aufnimmt, sich dort die einzelnen Beiträge holt und es erlaubt, diese zu lesen und selbst Beiträge zu schreiben. News-Server sind für bestimmte Regionen zentrale Rechner, welche die News-Datenbank halten, die in regelmäßigen Zeitabständen aktualisiert wird und welche für die Verbreitung von Artikeln sorgen. Sie können natürlich auch einen eigenen News-Server betreiben, der sich seine Daten wiederum von einem anderen News-Server holt. Es besteht dann auch die Möglichkeit, lokale Newsgruppen (d. h. firmeninterne Diskussionsforen) einzurichten.

## INTERNET - Möglichkeiten und Dienste

In News können die Beiträge von allen Benutzern gelesen und in der überwiegenden Zahl der Gruppen können auch eigene Artikel oder Antworten veröffentlicht werden. Dies eröffnet etliche neue Möglichkeiten. Man kann oft feststellen, daß Probleme (und deren Lösungen) anderer News-Benutzer auch für einen selbst von Interesse sind, und es bestehen bei eigenen Problemen gute Aussichten, daß einer der vielen Experten (die sogenannten 'Gurus' oder 'Wizards') relativ schnell weiterhelfen kann. Umgekehrt sollte man sich die Zeit nehmen, Fragen anderer News-Nutzer zu beantworten, denn das System funktioniert nur 'auf Gegenseitigkeit'. News ist deshalb auf keinen Fall nur eine kurzweilige Unterhaltung für Computer-Begeisterte, sondern eine ernst zu nehmende Informationsquelle und eine neue Möglichkeit, die wissenschaftliche Zusammenarbeit auf vielen Gebieten zu unterstützen. Darüber hinaus eröffnet News vollkommen neue Möglichkeiten der Publikation und der schnellen Diskussion innerhalb eines internationalen, offenen Teilnehmerkreises. Dies wird bisher zwar nur in speziellen Fachrichtungen genutzt, wird in Zukunft jedoch bestimmt auf breiteres Interesse stoßen. Wer sich schon gleich zu Beginn auf das Lesen weniger ausgesuchter Newsgruppen beschränkt, kann von Anfang an News als wertvolle Informationsquelle mit minimalem Zeitaufwand kennenlernen. Damit Sie sich nicht gleich als Anfänger outen, zunächst ein paar Fachbegriffe und weiter unten einige Verhaltensregeln:

Einige Begriffe (nach ihrer Wichtigkeit aufgeführt):

- Newsgroup:  
Die News-Gruppe ist ein Teilbereich von News, der einem bestimmten Thema gewidmet ist. In anderen Netzen heißen sie z. B. 'schwarze Bretter' oder 'Diskussionsforen'.
- News hierarchy:  
News-Gruppen mit verwandten Themen werden zu Familien zusammengefaßt, wodurch eine hierarchische Strukturierung der Gruppen entsteht.
- News Article:  
Die von den Benutzern verfaßten Beiträge zu einer News- Gruppe werden als News-Artikel bezeichnet.
- Newsreader:  
Benutzerschnittstelle für News, mit der i. a. Artikel gelesen, verfaßt, in einer Datei abgespeichert oder an einen anderen Benutzer per E-Mail geschickt werden können.
- Posten, Posting:  
Das Veröffentlichen eines News-Artikels wird als 'Posten' bezeichnet. Entsprechend wird ein News-Artikel oft auch 'Posting' genannt.
- Followup:  
Spezieller News-Artikel, der sich auf einen anderen Artikel bezieht. Der Followup übernimmt dabei i. a. den überschrift-Header des anderen Artikels und setzt dabei noch 'Re:' voran.

Historisch bedingt ordnet man die News-Hierarchien nach den folgenden Kriterien:

- Traditionelle (ursprüngliche), weltweit verbreitete News- Hierarchien. Diese Hierarchien gab es schon in der Anfangszeit, als News nur in der USA verfügbar war.
- Die restlichen (alternativen) Hierarchien, die weltweit gelesen werden können. Sie wurden im wesentlichen zu der Zeit gegründet, ab der News über die USA hinaus verbreitet wurde.
- Regionale Gruppen sind Gruppen, die i. a. nur von den News-Servern einer bestimmten Region geführt werden. 'Regional' kann sich dabei auf einen Kontinent, ein Land, ein Bundesland, eine Stadt, eine Institution, etc. beziehen.
- Lokale Gruppen sind nur für einen News-Server selbst oder für seine unmittelbare Nachbarschaft von Bedeutung. Zwischen 'lokal' und 'regional' gibt es i. a. keine scharfe Abgrenzung.

Die traditionellen News-Hierarchien

- comp:

## INTERNET - Möglichkeiten und Dienste

Themen, die mit dem Computer in Beruf, Wissenschaft und Forschung zu tun haben. Häufig existieren für Hardware und Software getrennte Gruppen.

- misc:  
In dieser Hierarchie werden Gruppen zusammengefaßt, die nicht in eine der anderen Kategorien passen oder die mehrere Gebiete streifen.
- news:  
Gruppen, die sich mit News selbst beschäftigen (Software, Administration, etc.).
- rec:  
Gruppen, für Hobbys und Freizeit.
- sci:  
Allgemeine wissenschaftliche Themen (z. B. Physik, Medizin, Philosophie).
- soc:  
Gruppen mit sozialen und kulturellen Themen.
- talk:  
Debattier-Gruppen.
- biz:  
Kommerzielles.
- alt:  
Die alternativen News-Hierarchien

Die Newsgroups sind hierarchisch geordnet. Unterhalb der oben angegebenen Hierarchien wird weiter verzweigt, wobei die einzelnen Hierarchiestufen durch Punkte getrennt werden. Bei landesspezifischen Gruppen wird das Länderkürzel vorangestellt, z. B. für deutschsprachige Gruppen 'de'; die deutsche Entsprechung von 'comp' ist somit 'de.comp'. Dann kann man weiter unterteilen, z. B. für die Diskussion über Computer-Betriebssysteme (operating systems) 'de.comp.os'. Nachdem es verschiedene Betriebssysteme gibt, entstehen dann Gruppen wie 'de.comp.os.linux', 'de.comp.os.minix', 'de.comp.os.os2', 'de.comp.os.unix', usw. Eine Unterteilung wird oft dann vorgenommen, wenn die Anzahl der täglichen Artikel in einer Newsgroup zunimmt und die Gruppe unübersichtlich wird. Die Newsgroupshierarchie 'de.\*' ist übrigens eine internationale deutschsprachige Hierarchie im Usenet. Es ist nicht die Deutschlandhierarchie, eine Hierarchie für Deutschland gibt es nicht.

Einige Newsgroups enthalten auch Binärdaten (Programme, Bilder, Sound-Dateien etc.). Sie sind durch den Begriff 'binaries' im Namen der Gruppe erkennbar (z. B. *comp.binaries.msdos*). Da nach wie vor 7-Bit-ASCII als kleinster gemeinsamer Standard für News und Mail gilt, lassen sich Binärdateien nicht ohne weiteres posten. Abhilfe schaffen hier die Programme UUENCODE und UUDECODE, mit deren Hilfe sich binäre Daten auf den Bereich der druckbaren ASCII-Zeichen (Großbuchstaben, Ziffern und Sonderzeichen) abbilden lassen. Es werden also Bytes in 6-Bit-Worten codiert und in Zeilen umbrochen. Die mit UUENCODE erzeugte Datei ist nun zwar größer als die Ursprungsdatei, sie läßt sich aber problemlos per News (oder Mail) verbreiten.

Das wachsende Newsaufkommen hat aber auch zu unschönen Erscheinungen geführt. Die Gruppen sind zwar thematisch untergliedert, aber man findet trotzdem immer mehr uninteressante Beiträge, endlose Streitereien um des Kaisers Bart oder Artikel, die überhaupt nicht zum Thema passen. Der Anteil an solchen nutzlosen Beiträgen wird oft in Analogie zur Störung beim Rundfunkempfang als 'Rauschen' bezeichnet. Das hat bei ständigen Newsbenutzern zu einer Absenkung der Toleranzschwelle geführt. Man muß bedenken, daß nicht nur das Lesen selbst Zeit kostet (selbst wenn man sich auf Überschriften beschränkt), sondern auch der Datentransport der News bis zum Rechner des Lesers in der Regel Telefonkosten verursacht. Wenn dann nur Unsinn zu lesen ist, reagieren die News-Benutzer irgendwann sauer. Insbesondere Nachrichten meist werblichen Inhalts, die in zahlreichen Diskussionsgruppen veröffentlicht werden und in keinem dieser Foren eigentlich einen Platz haben, lösen heftige Reaktionen (sogenannte 'flames') aus. Solche Massenveröffentlichungen haben den passenden Namen 'spam' (Sülze) erhalten. Das Rauschproblem hängt aber auch damit zusammen, daß viele Provider ihre Benutzer ohne jede Anleitung auf das Netz loslassen.

## INTERNET - Möglichkeiten und Dienste

Zum Schluß des Abschnitts möchte ich noch auf Newsgruppen hinweisen, die Informationen zu den verschiedensten Themen enthalten. Die wichtigsten sind *news.answers* und *de.newusers*. Dort finden Sie die sogenannten 'FAQ's (Frequently Asked Questions and Answers), in denen Antwort auf viele Fragen gegeben wird. Bevor man also eine Frage in den News losläßt, erst einmal in den FAQs stöbern. Sonst gibt es als Antwort auf eine Frage höchstens ein 'RTFM' (Read The Fucking Manual = Lies das Sch...-Handbuch) oder 'RTFAQ'. In Kapitel 4 wird das Thema News noch weiter vertieft. Ein Begriff sollte aber gleich noch geklärt werden, 'Usenet' User Network). News-Artikel und auch Mail sind nicht an das Internet gebunden, sondern können auch auf anderen Wegen, z. B. per Modem-Transfer, ausgetauscht werden (bei den News ist das durch die gewaltigen Datenmengen praktisch nur eingeschränkt möglich). Der Begriff 'Usenet' ist jedoch schwer zu fassen. Deshalb der Versuch einer Unterscheidung: Ein Internet ist eine Menge von Rechnern, die sich via IP ständig (!) untereinander verständigen können. Damit ist ein Internet ein Netz von sich technisch verstehenden Systemen. 'Ständig' ist auf definierte Zeiträume einschränkbar (für PPP und SLIP), heißt aber generell: jederzeit bis auf technische Pannen. Usenet-Rechner müssen darüberhinaus auch E-Mail senden und empfangen können. Dazu noch ein Zitat von Ed Krol aus seinem Buch 'Die Welt des Internet': *'USENET ist eines der am häufigsten mißverstandenen Konzepte. Es ist kein Rechnernetz. Es hängt nicht vom Internet ab. Es ist keine Software. Es ist eine Sammlung von Regeln, wie Newsgruppen weitergeleitet und verwaltet werden. Es ist außerdem ein Haufen Freiwilliger, die diese Regeln anwenden und respektieren. [...]. USENET besteht aus sieben gut verwalteten Newsgruppen-Hierarchien.'*

Auch wenn Newsgruppen sind nach wie vor großer Beliebtheit erfreuen, haben sie Konkurrenz bekommen. Die Web-basierten "Blogs" und "Wikis":

### **Blog**

"Blog" ist eine Wortkreuzung aus "World Wide Web" und "Logbook"). Es handelt sich um ein auf einer Webseite geführtes und damit öffentlich einsehbares Tagebuch oder Journal. Häufig ist ein Blog "endlos", d. h. eine lange, zeitlich umgekehrt sortierte Liste von Einträgen. Es handelt sich damit zwar um eine Website, die aber im Idealfall nur eine Inhaltsebene umfasst. Ein Blog ist ein für den Herausgeber ("Blogger") und seine Leser einfach zu handhabendes Medium zur Darstellung von Aspekten des eigenen Lebens und von Meinungen zu spezifischen Themengruppen. Es besteht oft die Möglichkeit auf die Beiträge zu antworten. Insofern kann es einem Internetforum ähneln, je nach Inhalt aber auch einer Elektronischen Zeitung.

Die ersten Weblogs tauchten Mitte der 1990er Jahre auf. Sie wurden Online-Tagebücher genannt und waren Webseiten, auf denen Internetnutzer periodisch Einträge über ihr eigenes Leben machten. Um 2004 wurde das "Bloggen" immer mehr kommerziell eingesetzt. Viele Online-Medien betreiben eigene Blogs, um ihren Leserkreis zu erweitern. D

### **Wiki**

Ein Wiki (Hawaiisch für "schnell") ist eine Sammlung von Webseiten, die von den Benutzern nicht nur gelesen, sondern auch direkt online geändert werden können. Wikis ermöglichen es verschiedenen Autoren, gemeinschaftlich an Texten zu arbeiten. Bekanntes Beispiel ist das Online-Lexikon Wikipedia. Wesentlich bei der meisten Wiki-Software ist die Versionsverwaltung, die es den Benutzern im Fall von Fehlern oder Vandalismus erlaubt, eine frühere Version einer Seite wiederherzustellen. Wie bei Hypertexten üblich, sind die einzelnen Seiten eines Wikis durch Hyperlinks miteinander verbunden. Das Konzept von Wikis ähnelt dem, was sich Tim Berners-Lee ca. 1990 ursprünglich unter dem WWW vorstellte. Die Informationen sollten am privaten Rechner verfügbar und sofort bearbeitbar sein. In historischer Perspektive beschreibt er dies in seinem Buch "Weaving The Web".

Wikis gehören zu den Content-Management-Systemen, setzen aber auf die Philosophie des offenen

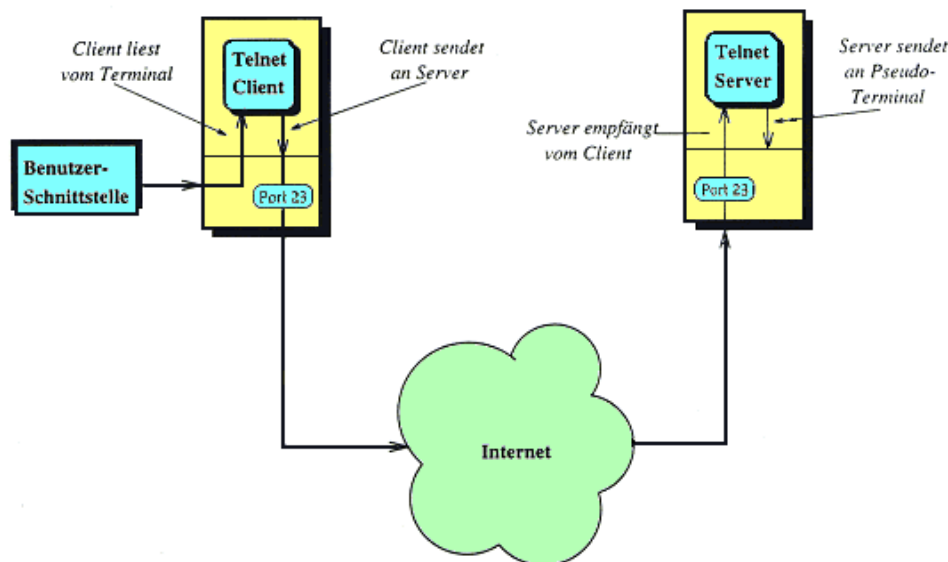
## INTERNET - Möglichkeiten und Dienste

Zugriffs, im Unterschied zu teils genau geregelten Arbeitsabläufen von Redaktionssystemen. Mit "offenem Zugriff" ist aber nicht gemeint, dass zwangsläufig jedes Wiki für alle lesbar oder schreibbar sein müsste, es kann sehr wohl Berechtigungen oder Beschränkungen für bestimmte Benutzergruppen geben.

Erste Wikis entstanden als Wissensverwaltungswerkzeuge von Architekten im Rahmen der Entwurfsmuster-Theorie. Das erste Wiki, WikiWikiWeb genannt, wurde vom US-amerikanischen Softwareautor Ward Cunningham ab 1994 entwickelt und 1995 übers Internet verfügbar gemacht. Das Wiki basierte auf Ideen aus HyperCard-Systemen, den Vorläufern des World Wide Web. Den Namen wählte Cunningham, da er bei der Ankunft am Flughafen auf Hawaii die Bezeichnung Wiki Wiki für den dortigen Shuttlebus kennengelernt hatte. Dabei übernahm er die Verdoppelung, die im Hawaiischen für eine Steigerung ("sehr schnell") steht.

### 2.3 Telnet

Zweck des Telnet-Programms ist, von einem beliebigen TCP/IP-fähigen Terminal einen interaktiven Zugang zu anderen Computern zu schaffen. Telnet = 'Teletype Network', zu deutsch etwa: 'Fernschreiber-Netzwerk'. Diese Programme gehen im einfachsten Fall von einem Text-Terminal aus und verwenden oft die VT100/VT200-Emulation.



Deshalb kann es bei Programmen zu Problemen kommen, die bildschirmorientiert arbeiten (z. B. Editoren). Für die Steuerung der Ausgabe, beispielsweise die Positionierung der Schreibmarke oder die Einstellung der Bildschirmfarbe, werden Steuerzeichen gesendet, welche die Terminal-Emulation 'verstehen' muß. Man hat also den gleichen Funktionsumfang wie ein lokal an dem jeweiligen Rechner angeschlossenes Terminal - egal wie weit der Rechner entfernt ist. Ist der Verbindungsaufbau erfolgreich, erscheint der Login-Prompt des fernen Rechners. Man kann sich prinzipiell an jedem Rechner im Internet einloggen - vorausgesetzt, man besitzt dort eine Zugangsberechtigung. Viele Rechner bieten jedoch auch einen Gastzugang. Es werden aber auch spezielle Informationsdienste angeboten. Um beispielsweise Whois-Anfragen abzusetzen, kann Telnet verwendet werden. Auch bieten manche Rechner über Telnet Zugang zu Multiuser-Spielen.

Primär dient Telnet aber dem Shell-Zugang auf einem fernen Rechner. Bei Shell-Zugängen verwenden Sie lediglich die Tastatur Ihres Computers, den "Rest" Ihres Computers brauchen Sie eigentlich gar nicht (so wie damals mit DOS beim PC). Sobald Sie die Verbindung zum fernen Rechner aufgebaut haben, können Sie all das auf dem Rechner machen, was man auch lokal an der Konsole machen kann. Je nach Betriebssystem (meist ist es UNIX) müssen Sie dessen Befehle lernen. Für den 'Normalnutzer' spielt Telnet eine untergeordnete Rolle, dagegen kann ein Administrator alle

ihm unterstehenden Computer bedienen, ohne seinen Arbeitsplatz verlassen zu müssen.

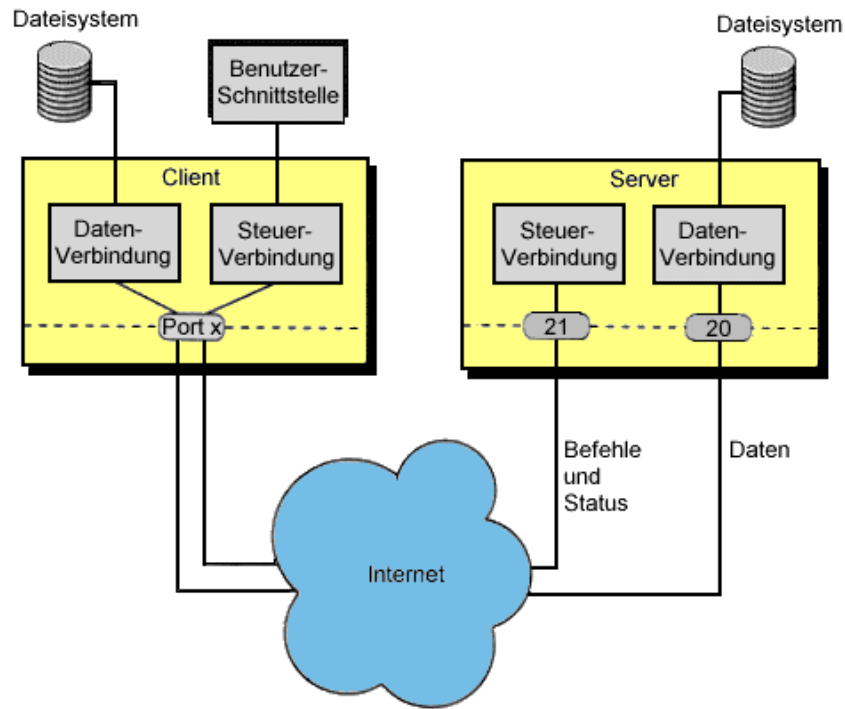
### 2.4 FTP (File Transfer Protocol)

Nehmen wir einmal an, Sie hätten noch immer kein vernünftiges Programm für die Nachbearbeitung Ihrer gescannten Bilder. Nachdem Sie in einer Newsgroup erkundigt haben, welches Programm für Windows das beste sei und nachdem man Ihnen einstimmig 'Paintshop Pro' empfohlen hat, starten Sie das FTP-Programm um Paintshop per FTP (File Transfer Protocol) von einem fernen Rechner zu holen. Damit es nicht noch länger dauert als ohnehin schon, kommt das Programm in Form einer einzigen Datei; alle Dateien des Programmpakets sind in einem sogenannten 'Archiv' zusammengepackt und die Daten komprimiert. Im Unterschied zu einer Telnet-Verbindung, die textorientiert ist, können mittels FTP beliebige Daten ausgetauscht werden (Bilder, Programme, Sounds, usw.).

Es gilt übrigens als ausgesprochen unhöflich, beispielsweise von München aus ein Programm in Hawaii abzuholen, wenn man es genausogut von Stuttgart bekommen kann (die Leitungen ins Ausland sind noch nicht so zahlreich, und man sollte deren Belastung möglichst gering halten). Benutzen Sie ausländische Server auch bitte zu Zeiten, wo diese wenig gebraucht werden, also ausserhalb der 'Bürostunden'. Meistens sieht man es der Internet-Adresse an, wo der entsprechende Server steht. Die wichtigsten Kennungen sind 'com', 'edu', 'gov', 'mil', 'net' und 'org' (siehe auch Kapitel 1). Server mit diesen Kennungen sind in der Regel in den USA stationiert (Zeitzone = Mitteleuropäische Zeit minus 6 bis 9 Stunden / Hawaii minus 12 Stunden), obwohl 'com'- und 'net'-Rechner überall auf der Welt stehen können. Andere Server erkennt man an der Länderkennung, z. B:

- at = Österreich
- de = Deutschland
- ch = Schweiz
- se = Schweden
- fr = Frankreich
- uk = England
- au = Australien (MEZ plus 8 Stunden)
- ca = Kanada (MEZ minus 6 bis 9 Stunden)
- jp = Japan (MEZ plus 8 Stunden)

## INTERNET - Möglichkeiten und Dienste



Der Verbindungsaufbau erfolgt wie bei Telnet, indem man dem FTP-Programm den gewünschten Zielrechner angibt. Bei erfolgreicher Verbindung kommt vom fernen Rechner wieder ein Login-Prompt. FTP funktioniert aber auch, wenn man auf dem fernen Rechner keine Benutzerberechtigung hat, denn viele Rechner bieten große Dateibereiche über sogenannten 'anonymen' FTP. Man gibt in diesem Fall als Benutzernamen 'ftp' (manchmal auch 'anonymous') ein und als Paßwort die eigene Mailadresse. Danach kann man sich im öffentlichen Dateibereich tummeln. Dazu braucht man nicht viele Kommandos.

- Mit '*cd <Verzeichnis>*' wechseln Sie in das entsprechende Unterverzeichnis.
- '*pwd*' zeigt Ihnen das aktuelle Verzeichnis an.
- Die Befehle '*ls*' oder '*dir*' ermöglichen die Anzeige des Verzeichnissesinhaltes.
- Mit '*get <Dateiname>*' holt man sich die gewünschte Datei und
- mit '*put <Dateiname>*' kann man lokale Dateien zum fernen Rechner übertragen.
- Mit '*quit*' beendet man die FTP-Sitzung.
- '*help*' liefert eine knappe Hilfestellung.

Noch etwas ganz Wichtiges: Das FTP-Protokoll kennt zwei Übertragungsmodi, den Transfer von Texten und von Binärdateien. Um die Daten auch korrekt zu bekommen, sollte man auf jeden Fall mit dem Kommando 'binary' in den Binärmodus schalten (Texte werden da natürlich auch korrekt angeliefert). Es gibt inzwischen, speziell bei Windows, auch etliche grafisch orientierte FTP-Clients, die sich automatisch das Inhaltsverzeichnis des fernen Rechners holen und dieses zusammen mit dem lokalen Verzeichnis wie in einem Dateimanager anzeigen. Hier kann man dann die Dateien per Mausklick hin- und hertransportieren.

Man kann eine zusammengefaßte Liste Hunderter von Anonymous-FTP-Sites erhalten, indem man eine E-Mail-Nachricht an *mail-server@rtfm.mit.edu* verschickt mit diesen Zeilen im Text der Nachricht:

```
send usenet/news.answers/ftp-list/sitelist/part1
send usenet/news.answers/ftp-list/sitelist/part2
...
send usenet/news.answers/ftp-list/sitelist/part13
send usenet/news.answers/ftp-list/sitelist/part18
```

## INTERNET - Möglichkeiten und Dienste

Dann erhält man per E-Mail 18 Dateien, die die "FTP Site List" enthalten. Jede dieser Dateien ist etwa 60 KB groß, die komplette Liste umfaßt also insgesamt mehr als 1 MB!

Nachdem Sie die Site-Liste erhalten haben, finden Sie etliche Einträge wie den folgenden - Site-Name, Ort und Infos über Dateien, die dort liegen, werden aufgeführt. Zum Beispiel:

```
Site:      oak.oakland.edu
Country:   USA
Organ:     Oakland University, Rochester, Michigan
System:    Unix
Comment:   Primary Simtel Software Repository Mirror
Files:     BBS lists; ham radio; TCP/IP; Mac;
           mode protocol info; MS-DOS; MS-Windows;
           PC Blue; PostScript; Simtel-20; Unix
```

### 2.5 SSH und SCP/SFTP

Telnet und FTP haben den Nachteil, dass bei beiden Benutzerkennung und Passwort im Klartext übertragen werden und damit abhörbar sind. Inzwischen wird weitaus häufiger Telnet durch SSH (Secure Shell) und FTP durch SCP (Secure Copy) oder SFTP (Secure FTP) ersetzt. Bei diesem Protokollen erfolgt die Übertragung aller Daten verschlüsselt.

### 2.6 IRC (Internet Relay Chat)

Nehmen wir nochmals das Beispiel mit dem Bildbearbeitungsprogramm. Sie möchten wissen, welches Programm sich für Windows am besten eignet. Diesmal plazieren Sie Ihre Anfrage jedoch nicht in einer Newsgroup, wo Sie auf eine Antwort warten müssen. Diesmal wollen Sie Ihre Frage sofort beantwortet haben. Dazu verwenden Sie den 'Internet Relay Chat' (to chat = schwatzen): Sie starten Ihr IRC-Programm und schalten auf den gewünschten Kanal (Channel), in Ihrem Fall am besten 'Windows'. Das Programm wird Ihnen anzeigen, wer noch alles auf diesem Kanal aktiv ist. An dieser Stelle ist ein Absatz zum Begriff 'Kanal' nötig.

Erst die Kanäle ermöglichen vernünftige Gespräche. Stellen Sie sich vor, einige tausend Teilnehmer schwatzen durcheinander. Kein Mensch könnte dem mehr folgen. Die Kanäle erlauben auch Grüppchen weniger Teilnehmer. Außerdem kann man bei vielen Kanälen schon am Namen erkennen, worüber diskutiert wird. Letztendlich kann jeder IRC-Teilnehmer auch einen eigenen Kanal eröffnen und nur bestimmte Teilnehmer zu einem privaten Schwätzchen bitten. Das IRC-Programm läßt Sie nämlich beliebige Kanäle öffnen, auch solche, die noch nicht existieren. Sie wären dann einfach der erste auf diesem Kanal und hätten automatisch Operator-Status.

Normalerweise meldet sich jeder mit einem Spitznamen ('Nickname') an. Sie sollten vorher das Handbuch zu Ihrem IRC-Programm studieren. Sonst wird man Sie bald als 'Newbie' entlarven und auch entsprechend behandeln. Allerdings gibt es im Internet auch viele nette Menschen, die sich gerade gegenüber einem Newbie besonders hilfsbereit zeigen. Eventuell können Sie einen Bekannten bitten, mit Ihnen den ersten 'Chat' auf einem privaten Kanal zu führen. Sie können dann auch die einzelnen Kommandos in Ruhe ausprobieren.

Nach Verbindungsaufnahme begrüßt Sie der Server mit einigen grundsätzlichen Informationen und Neuigkeiten. IRC wird hauptsächlich über eine textbasierte Eingabe gesteuert, was für Online-Gespräche am praktikabelsten ist. Die wichtigsten Befehle sind schnell gelernt, und man kann mit den meisten IRC-Clients auch zusätzlich Alias-Namen, also Abkürzungen, für die Befehle definieren.

Grundsätzlich beginnen alle Befehle mit einem Schrägstrich. Um einen Kanal auszuwählen, rufen Sie entweder mit `/list` eine Liste der verfügbaren Kanäle auf oder wechseln per `/join #Kanalname` direkt in einen Kanal. Nehmen wir an, Sie wollen in den Kanal `#irchelp` gelangen. Dazu müssen Sie `/join #irchelp` eingeben. Nun befinden Sie sich in einem Kanal, in dem Sie Hilfe zu Problemen mit IRC finden. Wollen Sie nun etwas zum Gespräch beitragen, müssen Sie Ihren Text lediglich eintippen und mit der Return-Taste abschließen, und schon erscheint die Zeile bei den anderen Teilnehmern des

## INTERNET - Möglichkeiten und Dienste

Kanals. Persönliche Nachrichten an einen Teilnehmer sendet man mit `/msg <nickname>`. Möchten Sie mehr über den IRC-Teilnehmer 'willy' erfahren, geben Sie `/ctcp willy finger` ein. Auf dem Bildschirm erscheint dann mehr Information über ihn. Die Informationen, die andere mit diesem Befehl über Sie erhalten, können Sie meist selbst unter `/ctcp finger reply` in Ihrem Client eintragen. Eine Liste der momentan auf Ihrem Server verfügbaren Kanäle erhalten Sie, wie oben schon erwähnt, mit dem Befehl `/list`. Diesen Befehl können Sie einschränken, indem Sie etwa mit `/list -min20` nur die Kanäle auflisten lassen, die mindestens 20 Teilnehmer haben. Oder Sie zeigen mit `/list #name` alle Kanäle, bei denen 'name' im Titel vorkommt. Übrigens kann es vorkommen, daß der Server nach dem List-Kommando die Verbindung beendet. Der Grund ist ein Schutzmechanismus im IRC, der verhindern soll, daß mehr Zeichen auf einmal übertragen werden, als man tippen kann. So kann niemand einen Kanal mit Texten blockieren, aber leider setzt dieser Mechanismus auch beim Auflisten der Kanäle ein. Abhilfe schafft da nur ein erneuter Connect (Verbindungsaufbau).

Wenn Sie einen eigenen Kanal ins Leben rufen, kommen auch Sie in den Genuß, einmal Operator zu sein. Die Gründung eines Kanals ist denkbar einfach. Sie müssen lediglich den neuen Kanal, beispielsweise 'blafasel', mit `/join #blafasel` aufrufen. In der Liste der Teilnehmer stehen zunächst nur Sie. Wenn Sie sich hier mit Freunden treffen möchten, sollten alle den gleichen IRC-Server verwenden, da neue Kanäle nicht immer auf die anderen Server übertragen werden. Nun können Sie loslegen und Ihren Kanal 'regieren'. Der wichtigste Befehl dabei ist `/mode #Kanal`, gefolgt von verschiedenen Parametern. Die Angabe des jeweiligen Kanals ist nur dann nötig, wenn Sie sich nicht in ihm befinden. Ein Pluszeichen vor einem Schalter aktiviert die jeweilige Funktion, ein Minus hebt sie auf. Mit `/mode #blafasel +s` machen Sie 'blafasel' einen geheimen Kanal, der in keiner Liste auftaucht. `/mode #blafasel +b <person>` etwa verbannt jemanden aus dem Kanal. Dabei wird die Person in der Form 'nickname!username@host' angegeben. Wer jetzt glaubt, einen Kanal namens blafasel gäbe es noch nicht, wird enttäuscht - zumindest auf dem Server in München.

Zum Schluß noch eine Warnung: Geben Sie keine Kommandos ein, die Sie nicht kennen. Es gibt nämlich auch die Möglichkeit, innerhalb des IRC Daten zwischen zwei Benutzern zu übertragen oder einem Benutzer gewisse Zugriffsrechte auf dem eigenen Rechner einzuräumen - jedenfalls genügend Möglichkeiten für einen kleinen Schabernack mit einem 'newbie'.

Die deutschen IRC-Server sind miteinander verbunden, Sie sollten sich also immer beim geographisch nächstgelegenen anmelden:

Aachen: irc.informatik.rwth-aachen.de  
Berlin: irc.fu-berlin.de  
Erlangen: ircserver.informatik.uni-erlangen.de  
Kaiserslautern sokrates.informatik.uni.kl.de  
Karlsruhe: irc.rz.uni-karlsruhe.de  
München: irc.informatik.tu-muenchen.de  
Paderborn: irc.uni-paderborn.de  
Rostock: irc.informatik.uni-rostock.de  
Stuttgart: irc.rus.uni-stuttgart.de

## 2.7 WWW (World Wide Web)

Diesen Dienst habe ich aus zwei Gründen bis zum Schluß aufgespart: Er ist die jüngste Erfindung im Netz und er integriert viele der anderen Dienste. Man kann deshalb fast alles mit nur einem Programm erledigen.

## INTERNET - Möglichkeiten und Dienste



Erfinder des WWW: Tim Berners-Lee

WWW wurde 1989 im CERN (dem Europäischen Kernforschungszentrum in Genf, Conseil Européen pour la Recherche Nucléaire) entwickelt, basierend auf einem System namens *Hypertext*. Stellen Sie sich ein Lexikon vor. Sie schlagen einen Begriff nach und finden dort auch Querverweise auf verwandte Begriffe. Ist das Lexikon einbändig, müssen Sie nur etwas blättern, um den angegebenen Querverweis zu finden. Bei einem mehrbändigen Lexikon müssen Sie unter Umständen einen anderen Band aus dem Regal nehmen. Handelt es sich beim Querverweis um eine andere Literaturangabe, ist möglicherweise ein Gang zur Bibliothek notwendig. 'Hypertext' bedeutet also, daß der Text Querverweise enthält, die man mit dem Betrachtungsprogramm per Tastendruck oder Mausklick abrufen kann. Das Hilfesystem von MS-Windows verwendet ein sehr einfaches Hypertextsystem. Nur geht WWW sehr viel weiter, es können nicht nur lokale Dateien, sondern Dateien auf beliebigen Rechnern im Internet als Querverweis angegeben und per Knopfdruck erreicht werden.

Aber das WWW ist nicht nur ein weiterer verbesserter Informationsservice wie Gopher oder WAIS, sondern es erlaubt auch die Einbindung von Bildern, Sounds oder Animationen in die Hypertext-Dokumente. Das Informationsangebot kann nun multimedial sein. Das hat letztendlich auch zur derzeitigen Popularität des Internet geführt; aber auch dazu, daß leider viele Menschen WWW und Internet gleichsetzen.

WWW ist aber auch der Versuch, die gesamte Information im Internet zusammenzufassen und über ein einziges Benutzerinterface zugänglich zu machen. Für den Benutzer existieren Programme verschiedener Hersteller, '*Browser*' genannt, die das WWW verfügbar machen. Die ausgewählten Wörter sind durch Farbe oder Unterstreichung hervorgehoben und können per Mausklick expandiert werden. Damit beginnt die Reise durch das WWW. Auf dieser Reise begegnen Sie unter Umständen recht unterschiedlichen Quellen des Internet (beispielsweise FTP, News, Telnet, Gopher, E-Mail). WWW ist dabei aber höchst flexibel und kann Ihnen sowohl einen FTP-Server als auch einen Telnet-Zugang, einen News-Reader oder weiteres komfortabel präsentieren, so daß es in naher Zukunft für viele Nutzer nur noch ein einziges Werkzeug geben wird, um im Internet zu recherchieren. Die einzelnen Informationsquellen werden durch *URLs* (URL = Unified Resource Locator) bezeichnet, die den gewählten Dienst und die Datenquelle (Rechner und Datei) angeben (siehe unten).

'Netscape Navigator', 'Internet Explorer', 'Opera', 'Hot Java' sind Programme zum Zugriff auf das WWW mit grafischer Benutzeroberfläche. Es gibt aber auch für einige Systeme textorientierte Browser, z. B. 'LYNX'. Wenn Sie das Programm starten, gelangen Sie automatisch in die 'Homepage' Ihres Systems (bzw. des Systems ihres Providers). Mit 'Homepage' wird normalerweise die Einstiegsseite eines WWW-Servers - oder auch eines Benutzers - bezeichnet. Von dort aus können Sie einfach durch Auswahl eines Querverweises mit der Maus oder den Cursortasten auf weitere Informationsseiten eines beliebigen Internetrechners wechseln, wobei der Verbindungsaufbau automatisch erfolgt. Woher die Information kommt, kann im Browser angezeigt werden. Aber nicht nur durch Unterstreichung und Farbe hervorgehobene Texte können als Link (so nennt man bei WWW die Querverweise) dienen, sondern auch Bilder, beispielsweise kleine Icons. Eine weitere Möglichkeit wird durch sogenannte 'Imagemaps' geboten. Hier kann der Benutzer beliebige Stellen auf einem Bild anklicken. Die Mauskoordinaten werden an den Informations-Server übertragen, und der kann entsprechend reagieren. Bei LEO (<http://www.leo.org/>) gibt es beispielsweise eine Deutschlandkarte, auf der man den gewünschten Zielort anklicken kann.

Wie Gopher basiert auch WWW auf dem Client-Server-Prinzip. Die Kommunikation erfolgt zwischen einem WWW-Server, der Informationen bereitstellt, und einem Client, der die Informationen anzeigt.

## INTERNET - Möglichkeiten und Dienste

Das Protokoll dafür heißt *HTTP* (HyperText Transfer Protocol). Mittels dieses Protokolls fordert der Client bei einem Server eine ganz bestimmte Datei mit einem Hypertext-Dokument an, die oft auch als '*WWW-Seite*' bezeichnet wird. Diese Datei wird dann vom Server an den Client übertragen und danach die Verbindung wieder geschlossen. Enthält das Dokument Bilder oder andere Multimedia-Teile, werden auch diese Datei für Datei übertragen. Weder Server noch Client 'merken' sich die Tatsache der Kommunikation (es gibt höchstens einen Eintrag in eine Protokolldatei auf dem Server). So ist jede Informationsanforderung ein abgeschlossener Vorgang. Etliche Browser können für ein Dokument, das aus mehreren Dateien besteht, auch mehrere Übertragungen parallel öffnen. Bilder bauen sich dann z. B. simultan auf. Dadurch wird aber auch die Belastung des Netzes erhöht. Damit Seiten, die öfter aufgerufen werden, nicht immer über das Netz transportiert werden müssen, können die meisten Browser WWW-Seiten lokal zwischenspeichern (Cache-Speicherung). Es erfolgt dann nur eine kurze Anfrage an den Server, ob sich die entsprechende Information seit dem letzten Zugriff geändert hat. Ist dies nicht der Fall, werden die Daten lokal von der Platte geholt. Die größeren Provider und Uni-Rechenzentren unterhalten ebenfalls ein Cache-System. Wenn ein Benutzer eine WWW-Seite anfordert, wird die Info auf der Platte des Providers zwischengespeichert. Bei der Anfrage eines weiteren Benutzers nach derselben Seite innerhalb eines bestimmten Zeitraums wird die lokale Kopie zur Verfügung gestellt ('Proxy-Cache', 'Proxy-Server'). Die Proxy-Software überprüft regelmäßig, ob sich die lokal gespeicherten Infos eventuell geändert haben und aktualisiert sie gegebenenfalls. Nicht mehr gefragte Seiten werden nach einiger Zeit gelöscht.

Die Browser selbst brauchen natürlich die Fähigkeit, nicht nur Text schön darzustellen, sondern auch Bilder anzuzeigen oder Töne abzuspielen. Für die gebräuchlichsten Dateiformate im WWW sind die entsprechenden Darstellungsprogramme im Browser integriert (z. B. für die Bildformate GIF und JPEG oder die Audioformate AU und WAV). Für andere Bildformate kann man dem Browser in einer Konfigurationsdatei mitteilen, welche externen Programme für bestimmte Dateiformate aufzurufen sind. Auf diese Weise kann man den Browser für beliebige Datenformate fit machen. Teilweise liefern auch schon die Browser-Hersteller solche Programme mit. Besonders komfortabel sind Programmen, die sich automatisch in den Browser einklinken (sogenannte '*Plug-In*'-Programme) Die Angabe des Anzeigeprogramms kann sogar interaktiv erfolgen. Stößt der Browser auf ein unbekanntes Dateiformat, wird der Benutzer gefragt, ob er ein Anzeigeprogramm angeben möchte oder ob die Datei für später auf der Platte gespeichert werden soll. In diesem Zusammenhang noch ein Hinweis: Alles was man beim Surfen im WWW auf dem Bildschirm sieht, ist in den lokalen Rechner übertragen worden und kann natürlich auch dauerhaft abgespeichert werden (File-Menü des Browsers, Menüpunkt 'Save as...'). Ebenso lassen sich die Bilder abspeichern (beim Netscape-Browser Mauszeiger auf das Bild ziehen, rechte Maustaste drücken).

Eigentlich ist das, was der Browser auf dem Bildschirm zeigt, die Wiedergabe einer Textdatei, die bestimmte Strukturierungsmerkmale enthält (probieren Sie mal den Menüpunkt 'view source' Ihres Browsers aus). Die Definitionssprache für solche Hypertext-Dokumente ist recht einfach, sie heißt HTML (HyperText Markup Language). HTML besteht aus normalem Text, bei dem Steueranweisungen, sogenannte HTML-'Tags', in den Text eingefügt werden. Diese Tags beeinflussen das Schriftbild, das später im Betrachtungsprogramm angezeigt wird; so gibt es zum Beispiel Tags, die einen Text als Überschrift kennzeichnen, oder Tags, die das Schriftbild verändern können. die Tags werden immer in '<' und '>' eingeschlossen. Mit nur wenigen Tags lassen sich schon sehr ansprechende Dokumente erstellen (siehe Kapitel 4).

Damit sind wir bei einem sehr wichtigen Punkt angelangt. HTML beschreibt die Struktur eines Dokuments, nicht dessen Aussehen! Denn der Informationsanbieter kann ja nicht wissen, ob der Leser seine Infos mit einem grafischen oder textorientierten Browser liest. Auch Bildschirmauflösung des Client-Computers, aktuelle Größe des Browser-Fensters, Farb- und Schriftwahl des Benutzers spielen eine Rolle. Manchen Benutzer schalten die Darstellung der Bilder ab, um Übertragungszeit zu sparen. All das sollte der Anbieter berücksichtigen (manche tun es, manche nicht). HTML ist eben kein Desktop-Publishing, sondern eine Struktursprache.

## INTERNET - Möglichkeiten und Dienste

Wie kommt man zu interessanten Informationen? Es gibt drei Möglichkeiten:

1. Durch Empfehlung von Bekannten (Es können auch Informationen aus den News sein). Jemand sagt also zu Ihnen: "Probiere mal: <http://www.fh-muenchen.de/>". Das tippen Sie dann ins Adreßfenster des Browsers, und schon landen Sie auf dem entsprechenden Computer, der Ihnen die gewünschte Information serviert.

2. Durch Netsurfen. Sie starten einfach irgendwo. Klicken Sie auf eines der Links, und Sie werden auf einem Server irgendwo in der großen weiten Welt landen. Die Chance ist groß, daß diese Web-Seite weitere Links enthält und so werden Sie von von Australien bis Japan springen und dabei ein paar interessante Dinge entdecken (und, falls Sie Ihr Datenvolumen bezahlen müssen, den nächsten Monat nicht mehr Netsurfen).

3. Durch Suchen. Ähnlich wie bei Gopher gibt es etliche Server, die mit Suchmaschinen einen Index vieler, vieler WWW-Server anlegen. In diesem Index kann man dann nach Stichworten suchen. Im Anhang sind einige Suchsysteme aufgelistet.

Oft hat man schon eine recht große Anzahl an Bildschirmen und WWW-Schritten hinter sich, bis man an der gewünschten Stelle oder interessanter Information angekommen ist. Um sich einen relativ langen oder umständlichen Weg bis zu dieser Stelle ein zweites Mal zu ersparen, kann man solche Stellen im WWW in der persönlichen 'Hotlist' eintragen.

Ein weiteres Merkmal des WWW ist die Schreiboption. Damit ist es möglich, Formulare, z. B. Bestellscheine von Bibliotheken oder Anmeldungen für Konferenzen, auszufüllen und abzuschicken. Diese Formulare werden dann von Programmen auf dem Server-Rechner bearbeitet. Diese schicken dann die Antwort wieder als WWW-Dokument zurück.

### Was ist ein URL?

URL ist die Abkürzung für 'Uniform Resource Locator' und wird im Netz verwendet, um Informationen vollständig zu bezeichnen. Mit einem URL wird nicht nur eine Datei und das zugehörige Verzeichnis, sondern auch der Rechner festgehalten, auf dem sie zu finden ist. Nachdem es im Internet verschiedene Dienste (z. B. FTP, Gopher, WWW) und somit verschiedene Protokolle gibt, wird schließlich noch die Zugriffsmethode festgehalten. Die allgemeine Syntax eines URL lautet also:

*Protokoll://Rechneradresse:Port/Dateipfad/Dateiname*

Ein URL besteht also aus vier Teilen, wobei nicht immer alle Teile aufgeführt werden müssen (meist ist z. B. keine Portangabe nötig). Beim Gopher-Protokoll wird statt Pfad- und Dateiname der Menütyp (01 fürs Startmenü) und ein Pfad angegeben. Das Protokoll gibt an, welcher Dienst genutzt werden soll, hier sind gebräuchlich:

- ftp - Dateitransfer mittels (anonymen) FTP  
z. B. <ftp://ftp.microsoft.com/pub/drivers/mouse/mouse.sys>
- gopher - Informationsrecherche auf einen Gopher-Server  
z. B. <gopher://gopher.dingsda.com>
- news - Lesen und Schreiben von News  
z. B. <news://news.lrz-muenchen.de/lrz.misc>
- http - Lesen von WWW-Seiten (http HyperText Transport Protocol)  
z. B. <http://lx-lbs.e-technik.fh-muenchen.de/index.html>
- mailto - Adresse für E-Mail  
z. B. <mailto:plate@e-technik.fh-muenchen.de>

## INTERNET - Möglichkeiten und Dienste

Die Portangabe hat einen sehr technischen Hintergrund. Um die einzelnen Dienste zu unterscheiden, wird beim TCP/IP-Protokoll (vereinfacht gesagt) jedem Dienst eine Nummer zugewiesen, eben die Port-Nummer. Es gibt allgemein festgelegte Ports, z. B. 80 für das http-Protokoll. Solche Standard-Ports müssen nicht angegeben werden. Man kann aber auch unbelegte Portnummern verwenden, beispielsweise um einen modifizierten WWW-Dienst anzubieten. In diesem Fall muß dann die Portnummer angegeben werden.

Sie sehen, ein URL ist ein nützliches Instrument, um Informationsquellen im Netz eindeutig zu bezeichnen. Inzwischen wird die Form der URL-Schreibweise nicht nur in WWW-Dokumenten, sondern auch ganz allgemein verwendet, um auf eine Ressource hinzuweisen, z. B. in einer E-Mail.

### 2.8 Ping

Dieses Programm ist ein kleines Tool, mit dem man feststellen kann, ob ein ferner Rechner überhaupt erreichbar ist. Ping variiert bei den verschiedenen Systemen, aber mit dem einfachen Aufruf

```
ping Rechnername
```

kann man den fernen Rechner 'anklingeln'. Je nach Programmversion erhält man nur die Meldung

```
Rechnername is alive
```

wenn alles in Ordnung ist - oder eine der Fehlermeldungen 'no answer', 'unknown host' oder 'network unreachable'.

```
PING wird ausgeführt für www.netzmafia.de [141.39.253.210] mit 32 Bytes Daten:
Antwort von 141.39.253.210: Bytes=32 Zeit=49ms TTL=252
Antwort von 141.39.253.210: Bytes=32 Zeit=36ms TTL=252
Antwort von 141.39.253.210: Bytes=32 Zeit=41ms TTL=252
Antwort von 141.39.253.210: Bytes=32 Zeit=38ms TTL=252

Ping-Statistik für 141.39.253.210:
  Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
  Ca. Zeitangaben in Millisek.:
    Minimum = 36ms, Maximum = 49ms, Mittelwert = 41ms
```

Bei anderen Versionen (oder durch Angabe des Parameters -s) erhält man für jedes Datenpaket eine Meldung. Das Kommando kann dann mit Ctrl-C abgebrochen werden, worauf eine Statistik ausgegeben und das Kommando beendet wird. Bei grafischen Benutzerschnittstellen erfolgt die Parameterangabe über Dialogfelder und nicht in der Kommandozeile.

### 2.9 Traceroute

Um festzustellen, welchen Weg die Datenpakete zu einem fernen Rechner nehmen und wie "gut" die Verbindung dorthin ist, kann man 'traceroute' einsetzen. Das Programm schickt UDP-Pakete mit unterschiedlicher "Lebensdauer" an einen unbenutzten Port und wertet so die Fehlermeldungen der einzelnen Router und Gateways aus. Dem Kommando wird wie bei Ping nur der Rechnername oder eine IP-Nummer als Parameter übergeben. Für jeden Gateway wird dann auf dem Bildschirm eine Zeile ausgegeben:

```
Zähler Gateway-Name Gateway-IP-Nummer "round-trip"-Zeit (3 Werte)
```

Traceroute sendet jeweils drei Datenpakete. Wenn auf ein Paket keine Antwort erfolgt, wird ein Sternchen (\*) ausgegeben. Ist ein Gateway nicht erreichbar, wird statt einer Zeitangabe '!N' (network unreachable) oder '!H' (host unreachable) ausgegeben. Man kann so feststellen, wo eine Verbindung unterbrochen ist, und auch, welchen Weg die Daten nehmen - wo also der Zielrechner in etwa steht. Bei grafischen Benutzerschnittstellen erfolgt die Parameterangabe über Dialogfelder und nicht in der

Kommandozeile.

```
C:\>tracert www.fireball.de

Route-Verfolgung zu www.fireball.de [193.7.255.22]
über maximal 30 Abschnitte:

 1  44 ms  39 ms  40 ms  ascend3.lrz-muenchen.de [129.187.24.125]
 2  40 ms  50 ms  41 ms  csr1cz.lrz-muenchen.de [129.187.24.254]
 3  37 ms  40 ms  44 ms  csrwan.lrz-muenchen.de [129.187.1.2]
 4  48 ms  42 ms  42 ms  ar-muenchen1.g-win.dfn.de [188.1.37.1]
 5  40 ms  42 ms  42 ms  cr-muenchen1.g-win.dfn.de [188.1.24.10]
 6  55 ms  55 ms  60 ms  cr-hamburg1.g-win.dfn.de [188.1.18.30]
 7  64 ms  59 ms  61 ms  zr-hamburg1.win-ip.dfn.de [188.1.3.213]
 8  57 ms  60 ms  61 ms  uni-hamburg1.win-ip.dfn.de [188.1.170.82]
 9  56 ms  68 ms  61 ms  kr-gruner-jahr.win-ip.dfn.de [188.1.3.2]
10  61 ms  59 ms  61 ms  194.153.105.1
11  61 ms  58 ms  54 ms  www.fireball.de [193.7.255.22]

Route-Verfolgung beendet.
```

## 2.10 Whois

Dieser Dienst liefert Informationen über Netzteilnehmer, sofern sich diese bei einem Whois-Server haben registrieren lassen. Das kann man über ein Formular, [netinfo/user-template.txt](http://netinfo/user-template.txt) auf [nic.ddn.mil](http://nic.ddn.mil), machen, das dann an [registrar@nic.ddn.mil](mailto:registrar@nic.ddn.mil) geschickt wird). Das Kommando lautet:

```
whois Namensangabe
```

wenn der voreingestellte Server verwendet wird. Mit Serverangabe lautet das Kommando:

```
whois -h Serverrechner Namensangabe
```

Man erhält dann alle Angaben aus der Datenbank, die zur Namensangabe passen. Als Namensangabe kann entweder ein Userpseudonym (Login-Name) oder der "echte" Name, eventuell als 'Nachname, Vorname', angegeben werden. Bei grafischen Benutzerschnittstellen erfolgt die Parameterangabe über Dialogfelder und nicht in der Kommandozeile.

Als Whois-Server können Sie 'whois.nic.de' oder 'whois.internic.net' angeben.

Durch die Namensangabe 'do Rechnerdomain' können Infos über die entsprechende Domain eingeholt werden. Ebenso kann man sich mit 'host Rechnername' über einzelne Computer oder mit 'net Netzwerknummer' über Netze informieren.

Fehlt das Whois-Kommando, eröffnet man eine Telnet-Verbindung zu [nic.ddn.mil](http://nic.ddn.mil) und gibt 'whois' nach dem @-Prompt ein. Auf den Prompt 'Whois:' hin kann man interaktive Anfragen absetzen (z. B. das 'help'-Kommando).

## 2.11 Java, Javascript, VRML, Flash etc.

Die Entwicklung der WWW-Browser schritt in den letzten Jahren rasant voran. Was mit der einfachen Darstellung von Texten mit der Einbindung von Multimedia-Elementen begann, entwickelt sich heute in Richtung 'virtuelle Realität' mit dreidimensionalen Darstellungen, Animationen und mehr.

### 2.11.1 Java

Mit Java hat SUN Microsystems etwas Neues geschaffen. Es können nun mit einer WWW-Seite nicht nur Text, Bilder, Sounds oder Animationen an den eigenen Rechner geliefert werden, sondern Programme, die lokal ablaufen. Statt beispielsweise ein Diagramm als Grafik zu senden, wird nun ein Diagramm-Zeichenprogramm mit den Daten geschickt. Um dann die Änderung der Daten kontinuierlich zu zeigen, müssen nun nur noch wenige Daten gesendet werden. Java ist eine richtige Programmiersprache, die an die Sprache C++ angelehnt ist. Wenn man im Browser eine Seite mit einem Java-Programm wählt, wird dieses Programm übertragen und dann von lokalen Browser ausgeführt.

## INTERNET - Möglichkeiten und Dienste

Der Ansatz für Java entstand noch unter der Prämisse, Java auf intelligenten Peripheriegeräten, z. B. beim interaktiven Fernsehen, einzusetzen. Eine logische Konsequenz daraus war der Wunsch nach Vereinfachung gegenüber existierenden Technologien und nach geringem Ressourcenverbrauch. C++ wurde daher schon recht früh als Programmiersprache verworfen. Um aber den Aufwand des Umstiegs für C-, Smalltalk- und Eiffel-Programmierer gering zu halten, entlehnt Java zum Teil deren Konzepte und legt die C++-Syntax zugrunde. Wichtige Unterschiede zwischen Java und C++ sind die Eliminierung der 'herkömmlichen' Zeiger, der zusammengesetzten und der vorzeichenlosen Datentypen. Neu (zumindest gegenüber C++) sind 'sichere' Arrays und vor allem ein Garbage Collector, der Speicherbereiche, die nicht mehr referenziert werden, automatisch freigibt. Die Java-Programme werden in ein kompaktes Format übersetzt, den Bytecode. Das ist an sich nichts neues, prinzipiell gab es das schon seit ca. 20 Jahren bei den BASIC-Interpretern der Heimcomputer. Im Java-fähigen Browser ist dann ein Interpreter für diesen Bytecode enthalten.

Der Interpreter überprüft den Bytecode vor der Ausführung auf unerlaubte Zugriffe auf Ressourcen. Auf diese Weise sind zwei Ausführungsmodi möglich: Einem lokal gestarteten Java-Applet (so nennt man die Java-Programme) kann der Benutzer den Zugriff auf den Rechner erlauben. Aus dem Netz geladene Applets behandelt Java dagegen äußerst mißtrauisch. Sie sind quasi in den Interpreter eingesperrt und verwenden genau definierte und vom Benutzer kontrollierte Möglichkeiten, beispielsweise auf die Festplatte zu schreiben. Zusätzlich wird jedes Applet vor und während der Ausführung auf korrekte Benutzung der Methoden und Instanzvariablen, mißbräuchliche Benutzung von Objektreferenzen, Stack-Überläufe und Zugriffsbeschränkungen getestet. Auch das Überschreiben von als sicher akzeptierten Klassen aus der lokalen Klassenbibliothek durch potentiell gefährliche Klassen aus dem Netz ist nicht ohne Erlaubnis des Benutzers möglich. Dies kann soweit gehen, daß der Benutzer jedes Laden einer externen Klasse bestätigen muß.

Für grafische Oberflächen, Ein-/Ausgabe, mathematische Operationen und Netzwerkfunktionen existieren vordefinierte Klassen. Ein Java-Programmierer muß nicht gleich alles wissen, die Einarbeitungszeit ist unter Java viel kürzer als unter C++. Eine Beschränkung der Programmiersprache auf spezielle Anwendungsgebiete ist (theoretisch) nicht vorgegeben. Was die Entwicklung vollwertiger Stand-alone-Programme angeht, gilt für Java jedoch das gleiche wie für andere plattformübergreifende Bibliotheken: es ist nur der 'kleinste gemeinsame Nenner' implementiert.

Für Java-Code, der in einem Web-Browser ablaufen soll, dient die Klasse 'Applet' als Ausgangspunkt. Im HTML-Code werden die Java-Klassen durch das <applet>-Tag eingebettet. 'Applet' definiert als Superklasse für alle Applikationen, die in Browser eingebettet werden sollen, auch einen Eventhandler für Benutzereingaben. Die wichtigsten Methoden für ein Applets sind die Initialisierung, Aktivierung der Anzeige, Deaktivierung der Anzeige und das Terminieren. Der Programmierer definiert in diesen Methoden das Verhalten des Applets auf der Seite. Gemäß dem 'Java-Knigge' sind Applets so zu programmieren, daß sie nur dann Rechenzeit beanspruchen, wenn die umgebende HTML-Seite angezeigt wird. Mit Java lassen sich auch komplette Bedienoberflächen programmieren. Die Möglichkeit, mit einem Mausklick ein Applet zu stoppen und wieder anzustarten, runden die Vorschriften ab. Um nicht den Browser mit der Interpretation des Applets zu blockieren und auch mehrere Applets simultan in einer HTML-Seite animieren zu können, sind Threads bereits Grundausstattung der Java-Laufzeitumgebung.

Wer sich für Java interessiert, findet Java-Seiten mit vielen Demos, den HotJava-Browser (für SUNs) und Java-Entwicklersoftware auf dem Server von SUN Microsystems unter <http://java.sun.com/>. Die Entwicklertools für Java-Applikationen stecken noch in den Kinderschuhen und sind zwar mächtig in der Leistung, aber noch recht unkomfortabel in der Bedienung.

### 2.11.2 JavaScript

JavaScript ist eine Script-Sprache mit begrenzten Fähigkeiten. Sie hat im Grunde mit Java nur einen Namensteil gemeinsam. JavaScript ist eine von Netscape entwickelte Programmiersprache. Die Sprache lehnt sich in der Syntax an die von Sun Microsystems entwickelte Programmiersprache Java an. JavaScript ist jedoch anspruchsloser im Aufbau als Java, eingeschränkter in den Möglichkeiten und für andere Zwecke gedacht. JavaScript ist im Gegensatz zu Java eine unmittelbare Ergänzung

## INTERNET - Möglichkeiten und Dienste

und Erweiterung zu HTML. JavaScript bietet sich für folgende Zwecke an:

- Animation (z. B. Marquees = Lauftexte programmieren) und in WWW-Seiten einbinden. Dabei steht Ihnen nicht nur das Anzeigefenster zur Verfügung, sondern auch Dialogbereiche des WWW-Browsers, etwa die Statuszeile.
- Projektsteuerung: Mit Hilfe von JavaScript lassen sich einige Lücken in HTML umgehen. So ist es mit Hilfe von JavaScript beispielsweise möglich, innerhalb eines Frame-Sets die Inhalte mehrerer Frame-Fenster gleichzeitig zu aktualisieren.
- Formularüberprüfung: Überprüfen der Anwendereingaben in einem HTML-Formular während der Eingabe
- Dynamische WWW-Seiten: Mit Hilfe von JavaScript läßt sich erreichen, daß sich WWW-Seiten während der Anzeige dynamisch verhalten. Beispielsweise Wechsel eines Bildmotivs, wenn sich die Maus über das Bild bewegt.
- Text generieren: Zur Laufzeit HTML-formatierten Text generieren, z.B. das aktuelle Datum und die aktuelle Uhrzeit anzuzeigen.
- Anwendungen: Mit Hilfe von JavaScript lassen sich einfache Anwendungen programmieren. Das können z.B. wissenschaftliche oder kaufmännische Taschenrechner sein. Auch einfache Spiele sind denkbar.

JavaScript-Programme werden im Gegensatz zu Java-Programmen direkt in der HTML-Datei notiert. Sie werden auch nicht - wie Java-Programme - kompiliert, sondern als Quelltext zur Laufzeit interpretiert, also ähnlich wie Batchdateien bzw. Shellscripts.

Dadurch bleibt JavaScript unkompliziert für den Programmierer, doch kritisch für den Anwender. Das Interpretieren von Quellcode ist ungleich langsamer als das Interpretieren von kompiliertem Code. Deshalb ist JavaScript nur für kleine und einfache Programmabläufe sinnvoll. Da kein Compilierungslauf und somit keine Fehlerprüfung stattfindet, gibt es bei JavaScript auch keinen Schutz vor schweren Programmfehlern.

Kleine Effekte, wie das bekannte Ändern des Erscheinungsbildes eines grafischen Elements, wenn die Maus darüber bewegt wird, lassen sich jedoch schnell realisieren.

### 2.11.3 VRML

Zur Beschreibung der WWW-Hypertext-Dokumente dient, wie erwähnt, eine Sprache namens HTML (HyperText Markup Language). Eine faszinierende Erweiterung für 3D-Grafiken ist die Beschreibungssprache VRML (Virtual Reality Modeling Language). Statt riesiger Animationsdateien werden auch hier nur Anweisungen geschickt, wie eine dreidimensionale Animation aussehen soll. Die so definierten Animationen werden dann auf dem lokalen Rechner erzeugt. Im Grunde ist dies keine grundlegende Neuerung, denn jedes Raytracing-Programm arbeitet mit einer solchen 3D-Sprache. Die Software berechnet anhand der Beschreibung die jeweilige Szenerie und stellt sie grafisch auf dem Bildschirm dar. VRML wird derzeit speziell auf die Bedürfnisse von WWW und Internet zugeschnitten, verfügt daher über spezifische Fähigkeiten, etwa die Einbindung von HTML-Dokumenten in 3D-Szenen. Die Entwicklung von VRML begann im Frühjahr 1994. Der Name VRML wurde damals geboren, allerdings noch als 'Virtual Reality Markup Language'.

Um nicht bei Null zu beginnen und statt dessen eine geeignete, bereits vorhandene 3D-Technologie zu nutzen, fiel die Wahl der Entwickler auf 'Open Inventor' von Silicon Graphics (SGI). Open Inventor unterstützt 3D-Szenarien mit Polygonobjekten, verschiedenen Belichtungsmöglichkeiten, Materialien oder Texturen. Zudem stellte SGI noch eine erste VRML-Parser-Library zur Verfügung, die als Grundlage für die Implementierung von 3D-Viewern diente.

### 2.11.4 Flash

Derzeit letzter Endpunkt der Technik auf Webseiten ist Flash. Web-Entwickler verwenden Flash zum Erstellen von attraktiven, auf Browsergröße anpassbaren, extrem kleinen und kompakten

## INTERNET - Möglichkeiten und Dienste

Navigations-Oberflächen, technischen Illustrationen, Langform-Animationen und sonstigen faszinierenden Effekte für Websites und andere Web-aktivierte Geräte (wie WebTV). Flash-Grafiken und -Animationen werden mit Hilfe der Zeichenwerkzeuge in Flash oder durch Importieren von Vektor-Grafiken erstellt. Flash unterstützt nicht nur Vektorgrafiken, die im Gegensatz zu Pixelgrafiken (GIF, JPEG, PNG, BMP, usw.) bei einer Skalierung (Vergrößerung oder Verkleinerung) ihr exaktes Aussehen behalten. Alle in Flash 4 erstellten Grafiken erscheinen auf dem Bildschirm nahtlos und glatt. Dank dieser Anti-Aliasing-Technik wirken die Designs immer ganz genau so, wie von ihrem Entwickler beabsichtigt. Zusätzlich unterstützt Flash Streaming-Verfahren. Damit lassen sich Animationen aller Art in WWW-Seiten einbinden - und nicht nur Zeichentrick-Filmchen, oder Textanimation, sondern auch Navigationselemente wie Schaltflächen und Menüs. Zur Bildanimation können dann noch die passenden Sounds hinzugefügt werden. Vektorbasierte Flash-Sites werden bereits beim Herunterladen abgespielt und machen so ein unmittelbares Feedback möglich. Flash eignet sich auch für Produktpräsentationen und ähnliche Aufgaben. Die Animationen lassen sich auch in gängige Videoformate (AVI, MPEG) umsetzen.



[Zum Inhaltsverzeichnis](#)



[Zum nächsten Abschnitt](#)

---

Copyright © Prof. Jürgen Plate, Fachhochschule München



## INTERNET - Möglichkeiten und Dienste

*Prof. Jürgen Plate*

---

# 3 Internet-Zugang und E-Commerce

*"Man kann die Menschen in zwei Kategorien einteilen. Solche, die Zugang zum Netz haben, und solche, die keinen haben."*

*Harley Hahn: A Students Guide to Unix.*

Wenn man Uni-, TU- oder FH-Angehöriger ist, stellt der Zugang kein Problem dar, man muß nur den Zuständigen für die Netzanbindung finden. Wenn man Mitarbeiter einer Firma ist, kann man ebensoviel Glück haben (insbesondere, wenn es eine Computerfirma ist).

Wenn beide Fälle für Sie nicht zutreffen, bleiben zwei Wege: Entweder, Sie überzeugen die Geschäftsleitung Ihrer Firma von den Vorteilen eines Internet-Zugangs oder Sie suchen sich einen Privatzugang. Das kann über sogenannte 'Service-Provider' oder Online-Dienste (z. B. auch AOL, T-Online) geschehen. Provider gibt es in nahezu jeder größeren Stadt und wer auf Reisen ist und nur kurz seine E-Mail lesen will, kann auch einen der 'Internet-by-call'-Anbieter in Anspruch nehmen, bei denen keine ANmeldung notwendig ist, weil die Abrechnung der Dienstleistung über die Telefongebühren erfolgt. Wer nur einmal schnuppern will, kann auch eines der vielen Internet-Cafes besuchen.

## 3.1 Die verschieden Arten des Zugangs

In Kapitel 1 wurde definiert, daß ein Rechner allgemein dann als zum Internet gehörend angesehen wird, wenn:

- er mit anderen Rechnern über TCP/IP kommunizieren kann
- er eine Netzadresse (IP-Nummer, siehe unten) besitzt
- er mit anderen Rechnern kommunizieren kann, die eine Netzadresse haben

Man kann die Zugehörigkeit zum Internet aber noch etwas weiter klassifizieren. RFC 1775 unterscheidet vier verschiedene Arten/Stufen des Internet-Zugangs:

### 1. Full Access

Der Rechner ist über Standleitung angebunden und arbeitet als Client und Server. Der Benutzer kann alles was denkbar ist. In der Regel nur für Hochschulen und Firmen realisierbar. Notwendig, wenn man Informationsanbieter werden will.

### 2. Client Access

Der Rechner hat einen Einwahl-Zugang über Telefonleitung (Modem), ISDN oder DSL (Digital Subscriber Line, z. B. T-DSL). Es wird ein serielles Internet-Protokoll verwendet (SLIP/PPP). Der Rechner verwendet eine passende Software-Schnittstelle des Betriebssystems (z. B. das DFÜ-Netzwerk bei Windows) und ist nur solange im Netz präsent, wie die Wahlverbindung besteht. Für Firmen mit rein passiver Nutzung (z.B. E-Mail empfangen und versenden) und den Privatmann ist dieser Zugang interessant. Bei ISDN und DSL ist der Übergang zum 'Full Access' gleitend, da hier die Leitung innerhalb von Sekunden steht.

### 3. Mediated Access

Der Benutzer hat einen Online-Account. Auf dem lokalen Computer läuft ein Terminalprogramm, mit dessen Hilfe eine temporäre Verbindung zum Provider über Telefonleitung (Modem), ISDN oder DSL unterhalten wird. Das System verhält sich wie ein Terminal am eigentlichen Internet-Rechner. Zusätzlich ist meist ein Datentransfer möglich. Für Firmen, die nur E-Mail betreiben und den Privatmann. WWW-Zugang kann meist nur im Textmodus erfolgen. Ein früher häufiger, heute eher seltener Fall.

### 4. Messaging Access

## INTERNET - Möglichkeiten und Dienste

Es handelt sich um einen Teilzugang für E-Mail und News. Die Nachrichten werden offline erstellt bzw. gelesen. Die Daten werden dann als Block zu einem fernen Rechner übertragen (per Modem oder ISDN). Das Protokoll ist meist UUCP (Unix-to-Unix-Copy). Das funktioniert aber sogar noch im finstersten Urwald (sofern man sein Satellitentelefon dabei hat).

Nicht alle Formen des Zugangs lassen sich leicht in die o. g. Gruppen leicht einordnen. Beispielsweise bietet die Telekom seit September 95 über T-Online einen Zugang zum Internet für WWW und E-Mail - sofern man die spezielle Zugangssoftware von T-Online benutzt. Da aber eine PPP-Verbindung aufgebaut wird, kann man mit externen Programmen auf alle Dienste, z. B. FTP oder IRC zugreifen. Das ist einerseits ein Mediated Access (T-Online-Software), andererseits ein Client Access (andere Software).

Der Messaging Access ist übrigens gar nicht so schlecht, wie man zunächst denken mag. Es gibt etliche Rechner, welche andere Internet-Dienste über E-Mail anbieten. So kann man sich z. B. von manchen FTP-Servern Dateien per E-Mail schicken lassen, wenn man FTP nicht nutzen kann. Selbst Gopher- oder WWW-Dokumente kann man sich so schicken lassen und dann auf dem lokalen Rechner ansehen.

Man kann den Zugang noch nach der Dauer der Verbindung klassifizieren:

- ◆ Wählleitung (Telefonverbindung): über Einwahlknoten zu Provider, wie unten beschrieben. Einige Provider bieten als sogenannte "Flatrate" einen Wählzugang zum monatlichen Pauschaltarif an.
- ◆ Standleitung: direkter Zugang, z. B. über Hochschulen, Forschungseinrichtungen, große Firmen oder Provider. Die Kosten für eine Standleitung der Telekom liegen teilweise unter den Gebühren einer Wählleitung bei intensiver Nutzung. Der Provider muß aber eine Standleitung unterstützen.

Typische Geschwindigkeiten für Verbindungen:

- ◆ 28,8 kb/s bis 57,6 kb/s bei schnellen Modemverbindung
- ◆ 64 kb/s oder 128 kb/s (ISDN)
- ◆ 2 Mb/s bis 34 Mb/s über Provider

### 3.2 Internet-Provider

Ein Anteil der Internet-Kosten wird derzeit noch von Regierungsstellen und Hochschulen bezahlt. Es gibt aber inzwischen viele kommerzielle Netzbetreiber, sogenannte 'Provider', die natürlich für Leitungskosten, etc. bezahlen müssen und diese Kosten an den Kunden weitergeben. In den USA werden mittlerweile mehr als die Hälfte der Internet-Kosten von kommerziellen Organisationen getragen. Man kann unterscheiden zwischen:

- ◆ Vereine für private Anwender
- ◆ Kommerzielle Provider für private und kommerzielle Anwender
- ◆ DFN-Verein (Deutsches Forschungsnetz) als Betreiber des Wissenschaftsnetzes

Je nach Provider zahlt man entweder für die Online-Zeit oder für das transportierte Datenvolumen. Hinzu kommen die Telefonkosten für die Modem- oder ISDN-Verbindung zum Provider. Dieser sollte sich darum im Nahbereich befinden. Viele Provider unterhalten mehrere Einwahlpunkte in ganz Deutschland (POP Point Of Presence).

Die Kosten liegen zwischen ca. 15 Mark/Monat (E-Mail, WWW und News) bis hin zu mehreren tausend Mark (Standleitung). Mittlerweile gibt es auch Angebote, bei denen die Online-Zeit und die Telefonkosten über einen einzigen Minuten-Tarif abgerechnet werden. Für Vielsurfer sind die 'Flat-Rate'-Angebote interessant. Hier werden Verbindungskosten und Online-Gebühren über eine Monatspauschale abgegolten. Aber Vorsicht: Je nach Anbieter gibt es trotzdem Einschränkungen, z. B. darf nur ein einziger Computer online sein oder es

## INTERNET - Möglichkeiten und Dienste

sind nur Privatkunden zugelassen. Bei manchen Angeboten ist die Gesamt-Onlinezeit pro Monat begrenzt, andere schalten aus technischen Gründen einmal alle 24 Stunden offline.

### Einige Unterschiede zwischen Providern

- ◆ Preis
  - ◇ Grundgebühr für die Bereitstellung des Zugangs
  - ◇ Gebühr für die Dauer einer Verbindung
  - ◇ Gebühr für übertragenes Volumen
  - ◇ Pauschale, ggf. sogar inklusive der Telefongebühren
- ◆ Geschwindigkeit
  - ◇ Anzahl und Geschwindigkeit der Leitungen in Deutschland
  - ◇ Anzahl und Geschwindigkeit der Übergangspunkte zu übergeordneten Providern in anderen Ländern
- ◆ Qualität
  - ◇ Zuverlässigkeit
  - ◇ Stabilität
  - ◇ Lastverteilung
  - ◇ Verfügbarkeit
- ◆ Zusatzleistungen
  - ◇ Bereitstellung einer Mailadresse und eines Postfaches
  - ◇ Bereitstellung eines Domain-Namens
  - ◇ Bereitstellung von Webespace
  - ◇ FTP-Zugriff
  - ◇ Shell-Zugriff
- ◆ Dienstleistungen
  - ◇ Bereitstellung von Software
  - ◇ Erstellen von Web-Seiten
  - ◇ Datenbankanbindung, Softwareerstellung
  - ◇ Server-Hosting
  - ◇ Hilfe bei Problemen

### 3.3 Hardware, Software und Betriebssysteme

Der Privatanwender wird meist mit einem Wählanschluß die Verbindung zum Internet aufnehmen. Was ist dazu nötig?

1. Computer:  
Grundsätzlich ist die Teilnahme am Internet nicht an bestimmte Computer oder Betriebssysteme gebunden. Es ist nur so, daß es auch manchen Systemen einfacher geht, als auf anderen. So sind z. B. Unix- und Linux-Workstations von vorne herein mit Software für TCP/IP und Internet-Dienste ausgerüstet.
2. Modem oder ISDN-Karte:  
Beide Methoden sind heute nahezu gleichwertig. Man richtet sich da nach der installierten Telefon-Einrichtung. Für ISDN genügt eine passive ISDN-Karte (z. B. die AVM Fritz-Karte). Bei Modems ist eine Übertragungsgeschwindigkeit von 56 kBit/s nach dem V.90 Standard zu empfehlen, auch wenn man nicht immer die volle Geschwindigkeit erreicht.
3. Provider:  
Der Provider stellt Zugangskennung sowie Telefonnummer zur Einwahl und damit den Anschluss an das Internet zur Verfügung (siehe oben).
4. Software zur Verbindung mit dem Internet:  
Bei Windows 95/98/NT ist das erforderliche DFÜ-Netzwerk bereits im Betriebssystem vorhanden (*winsock.dll*). Die Installation dieser Software ist

## INTERNET - Möglichkeiten und Dienste

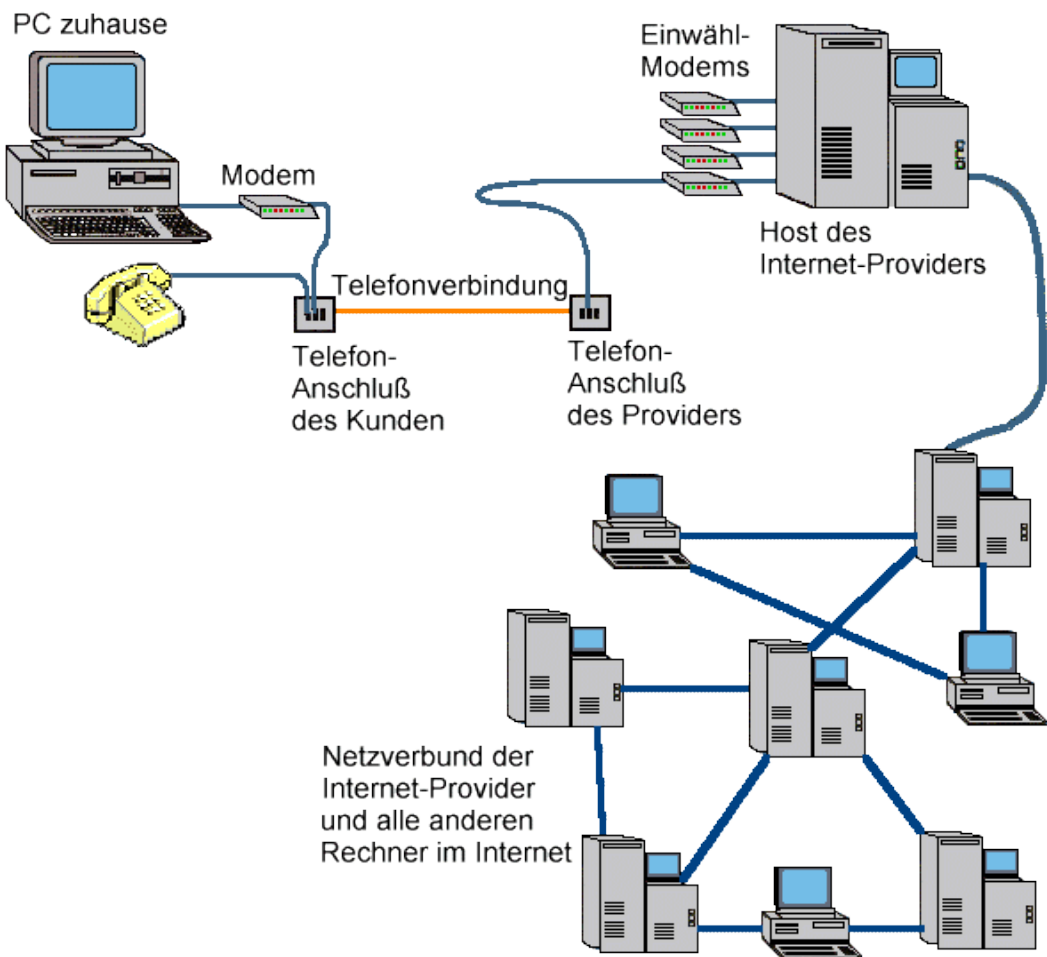
manchmal etwas knifflig. Ebenso gibt es passende Tools für den Mac von Apple. Auch für exotischere Systeme (IBM OS/2, Commodore Amiga, etc.) gibt es etwas. Generell geben hier auch die Provider Tips oder bieten passende Softwarepakete an. Sobald die Software zur Einwahl funktioniert, besteht eine SLIP- (Serial Line Internet Protocol) oder PPP- (Point to Point Protocol) Verbindung, d.h.:

- ◊ Vom Provider wurde eine temporäre IP-Adresse zugeteilt.
- ◊ Der lokale Rechner funktioniert so, als wäre er fest mit dem Internet verbunden.

Standleitungsverbindungen und Großrechneranbindungen erfordern vielfältige und teilweise spezielle Maßnahmen, hier kann ich keine allgemeinen Hinweise geben.

### 5. Software zur Nutzung von Internet-Diensten:

Aufruf eines Programmes zur Nutzung von Internet-Diensten, z. B. einen Browser für WWW, einen FTP-Clienten, ein E-Mail-Programm, usw. Einfache Programme für Telnet, FTP, Ping, Traceroute sind bereits in Windows enthalten, ebenso der Internet-Explorer (Browser). Komfortablere Software findet man im Freeware- und Sharewareangebot. Auch bei Linux sind alle notwendigen Clients bei allen Distributionen dabei.



Dünner ist die Software-Decke, wenn man Anbieter werden will, z. B. selbst WWW-Seiten oder FTP-Dienste anbieten. Dann muß die Leitung zum Provider zumindest eine ISDN-Verbindung sein (entweder permanent oder 'on demand'). Für den Windows NT Server gibt es das Back-Office-Paket. Ideal ist für einen Anbieter-Rechner jedoch das Betriebssystem Unix. Es handelt sich um ein Multiuser- und Multitasking-Betriebssystem, das auch

entsprechende Sicherheitskomponenten enthält. Zudem ist die Entwicklung des Internets eng mit der Entwicklung von Unix verbunden. Inzwischen gibt es auch zwei frei erhältliche Unix-Systeme, 'Linux' und 'Free BSD', die stabil laufen und alles bieten, was das Herz begehrt. Nicht zuletzt wegen der freien Verfügbarkeit der Programmquellen sind diese Betriebssysteme auch bei den Internet-Provider sehr beliebt. Wer als Anbieter mehr als nur statische Seitenangebote machen will (z. B. Datenbankanbindung, Fax-Gateway usw.), sollte sich mit Linux vertraut machen. Übrigens - so schwer, wie manche Leute sagen, ist die Bedienung von Unix gar nicht zu erlernen.

### 3.4 Verhalten im Internet

Da das Internet ein 'Netz der Netze' ist, gibt es von Region zu Region unterschiedliche Benutzungsregeln, die den Gebrauch bestimmen. Große Teile des Internets werden von der öffentlichen Hand bezahlt, so daß z. B. der kommerzielle Gebrauch dieser Netze von vorneherein beschränkt sein muß. Das Deutsche Wissenschaftsnetz WiN, betrieben von der Deutschen Bundespost Telekom, wird bezahlt vom Verein zur Förderung eines Deutschen Forschungsnetzes (DFN-Verein) durch die Anschlußgebühren, die Mitglieder des Vereins entrichten. Finanziert wird der Verein hauptsächlich durch das Bundesforschungsministerium und die Beiträge seiner Mitglieder. Das sind zum größten Teil die deutschen Universitäten, aber auch Forschungsabteilungen von Firmen. Der Gebrauch des WiN ist also zu Forschungszwecken auch kommerziellen Einrichtungen erlaubt. Rein kommerzielle Zwecke wie Werbung, Angebots- und Rechnungsstellung sind dagegen im WiN nicht gestattet. Die Grauzone ist hier natürlich beliebig groß. Ähnliche Strukturen findet man überall im Internet. So wurde in den USA vor ein paar Jahren beschlossen, die bis zu diesem Zeitpunkt parallel gefahrenen Netzwerke jeder Bundesbehörde im Bereich Lehre und Forschung (NFSNET, NASA Science Internet, ...) zusammenzulegen, um das NREN zu bilden (National Research and Education Network). Das Netz darf zu Zwecken der Forschung und Lehre oder der Unterstützung der Forschung und Lehre verwendet werden. Dieser zweite Teil ist sehr wichtig, da er Firmen erlaubt, Kundenkontakte zu Forschungsinstitutionen zu pflegen. Aber nicht nur die öffentlichen Investitionen zählen hier, sondern auch der Arbeitsaufwand und Kreativität von Fachleuten sowohl im öffentlichen Bereich als auch in der Wirtschaft. So dauern beispielsweise die Abstimmungsprozesse in der internationalen Standardisierung seit mehreren Jahrzehnten an. Dazu kommt die tagtägliche sorgfältige Pflegearbeit im weltweiten Verbund.

Auch für den einzelnen, 'authorisierten' Benutzer gibt es einige Dinge beim Gebrauch des Netzes zu beachten. Der Aufbau des Internet läßt sehr viel Raum für Individualismus, birgt aber gleichzeitig auch viele Gefahren für Mißbrauch. Die Nutzung des Netzes unterliegt daher rechtlichen und ethischen Grundsätzen. So selbstverständlich, wie manche meinen, ist der freie Zugang zum Internet nämlich nicht. Nicht immer ist die persönlich optimale Nutzung auch global optimal. Gerade mit der derzeit rapide wachsende Zahl der Internet-Nutzer kann der Ausbau der Netz-Infrastruktur nicht immer Schritt halten. Jeder Teilnehmer sollte darauf achten, daß die Netzbelastung in vertretbaren Grenzen bleibt. Der Mißbrauch selbst durch eine kleine Gruppe von Netznutzern könnte das Ansehen der Netze in ihrer Gesamtheit schädigen. Die Netze sind relativ einfach zu nutzen: Mit nur wenigen Kommandos kann ein Datentransfer rund um den Globus oder ein Nachrichtenaustausch mit einer großen Zahl von Partnern ausgelöst werden. Leicht verkennt der Nutzer die Komplexität der von ihm ausgelösten Netzaktivitäten. Er sollte daher vorsichtig mit Netzaufrufen umgehen. Ein Beispiel für leichtfertigen Gebrauch stellt die Vergeudung von Ressourcen durch einen zwar autorisierten, aber unbedachten Umgang mit den Netzdiensten dar; dies gilt insbesondere für den Abruf von Daten aus den USA, wenn diese in Deutschland bereits verfügbar sind. Formen einer unsachgemäßen Nutzung sind:

## INTERNET - Möglichkeiten und Dienste

- ◆ der Versuch, ohne ausdrückliche Autorisierung Zugang zu Netzdiensten - welcher Art auch immer - zu erlangen
- ◆ die Verletzung der Integrität von Informationen, die über die Netze verfügbar sind
- ◆ der Eingriff in die individuelle Arbeitsumgebung eines Netznutzers
- ◆ jede Art des Mithörens von Datenübermittlungen, des Stöberns in fremden Datenbeständen oder der Weitergabe von unabsichtlich erhaltenen Angaben über Rechner und Personen
- ◆ Unbeabsichtigte, exzessive Nutzung des Netzwerkes durch fehlerhafte oder unangepaßte Anwendungen. Beispiele hierzu sind:
  - ◇ Unendlich sich wiederholende Abfragen an Server mit falschen Adressen
  - ◇ Einbinden von fremden Dateisystemen in das eigene über WAN mit NFS
  - ◇ Intensives Betreiben von Netzwerkspielen
- ◆ Moralisch verwerfliche Nutzung durch:
  - ◇ Verbreitung gewaltverherrlichenden oder diskriminierenden Gedankengutes
  - ◇ Verbreitung sexistischen Materials

Vielfach führen die Anwendungen zu einer Belastung des Netzes, die von anderen Netzwerkbenutzern oder den Systemverwaltern nicht unbemerkt bleibt. In der Regel folgt eine freundliche Mitteilung an den Verursacher, die störende Netznutzung zu unterlassen. Falls keine Reaktion erfolgt, wird man sich noch öfters bemühen, mit dem Nutzer ins Gespräch zu kommen, bis vom zuständigen Systemverwalter der Zugang zum Internet für diesen Nutzer im Interesse der anderen gesperrt werden muß. Zum Schluß einige Verhaltensregeln:

- ◆ Schützen Sie den Zugang zu Ihrem Rechner, indem Sie ihr(e) Paßwort(e) geheim halten und regelmäßig wechseln.
- ◆ Beachten Sie die Verhältnismäßigkeit Ihres Tuns in Hinblick auf den zu erreichenden Zweck.
- ◆ Trotz allem sind Störungen nicht auszuschließen. Üben Sie daher die nötige Toleranz.

### 3.5 Kommerz im Internet

Landauf, landab wird den Entscheidern in den Unternehmen erzählt, wie wichtig es ist, sich auf Online-Kommunikation vorzubereiten (richtig!), daß man mit Internet sehr einfach Geld verdienen kann (falsch!), weil 100 Millionen Internet-Benutzer nur darauf warten, auf den multimedialen WWW-Seiten der Unternehmen Geld auszugeben (auwei!). Auch auf die Gefahr hin, als Spielverderber zu gelten, zunächst ein paar Warnungen und dann die positiven Seiten:

#### 3.5.1 Warnungen (was nicht geht)

- ◆ Das Internet ist aus einer anarchischen Goodwill-Struktur auf Gegenseitigkeit entstanden. Auch wenn es heute so scheint, als seien die kommerziellen Anwendungen der primäre Inhalt des Internet, so täuscht das. Wie schon im ersten Kapitel gesagt, sollte man Internet (das Transportmedium) und WWW (einer von vielen Internet-Diensten) nicht in einen Topf werfen. Wer hier besonders schlau sein will, bekommt schnell Ärger. Aktive Werbung hat im Internet (speziell in den Newsgruppen oder als E-Mail) etwa das gleiche Image wie Kakerlaken: Man meidet sie, wo man kann, die Initiatoren werden bestenfalls geächtet, schlimmstenfalls beschimpft und bekämpft. Das liegt auch daran, daß noch immer viele Teilnehmer das Datenvolumen oder die Übertragungszeit bezahlen müssen - also auch die unverlangt zugesandte Werbung.
- ◆ Das Internet ist noch nicht besonders gut darauf ausgelegt, Geldgeschäfte zu tätigen. Näheres dazu weiter unten.
- ◆ Das 'World Wide Web' ist zwar theoretisch multimedial, bleibt aber im Kern eine Hyperlink-Oberfläche eines für Textübertragung ausgelegten Netzes. Die in den Text

## INTERNET - Möglichkeiten und Dienste

eingestreuten Bildchen und Animationen ändern auch nichts an dieser Tatsache. Große Bilder und Textdateien erfordern für nicht optimal angebundene Teilnehmer lange Übertragungszeiten und machen so die WWW-Seiten uninteressant.

### 3.5.2 Vorteile der Internet-Nutzung:

- ◆ Über E-Mail kann man schnell und einfach mit Kollegen und Kunden kommunizieren. Im Gegensatz zum Fax kann der Empfänger die Daten gleich im Computer weiterverarbeiten. Je mehr Firmen über E-Mail erreichbar sind, desto höher ist die Chance, per E-Mail Bestellungen (Ein- und Verkauf) abzuwickeln. Vertreter können per E-Mail mit der Zentrale in Kontakt bleiben. Bei Internationalen Firmen entfällt das Problem der Zeitverschiebung.
- ◆ Supportleistungen sind schnell an den Kunden zu bringen (E-Mail, FTP- oder WWW-Server). Aber Vorsicht, ein schlecht gepflegtes Angebot schadet mehr als gar keines. Das Netz bietet die Möglichkeit, eigene Informationen zu veröffentlichen.
- ◆ Durch Beobachten des Netzes können Koperationspartner oder auch neue Entwicklungen erkannt werden. Zahllose WWW- und FTP-Server bieten Software aller Art (auch als Quelle) und massenhaft Dokumente.
- ◆ Die Geschwindigkeit, mit der Informationen verbreitet werden können, läßt sich von keinem anderen Medium erreichen. Sobald die Info auf dem eigenen WWW- oder FTP-Server bereitliegt, ist sie auch weltweit abrufbar.

### 3.5.3 Tips für Internet-Unternehmer

- ◆ Schauen Sie sich an, was der Mitbewerber so treibt.
- ◆ Holen Sie Angebote von verschiedenen Providern ein. Manchmal ist eine höhere Monatspauschale günstiger, als eine Rechnungstellung nach Zeit oder tatsächlich übertragenen Daten.
- ◆ Es reicht nicht, sich im Netz zu präsentieren. Wichtig sind:
  - ◇ ansprechende, speicheroptimierte WWW-Seiten (keine Riesenbilder)
  - ◇ stimmiges, durchgängiges Konzept
  - ◇ gute Öffentlichkeitsarbeit
  - ◇ passendes Umfeld
- ◆ Ist die Homepage fertig, dann sollte man sie bei allen einschlägigen Suchmaschinen und -Verzeichnissen registrieren.
- ◆ Online-Seiten leben von der laufenden Aktualisierung.
- ◆ Auf Anfragen sofort reagieren, sonst ist der Kunde enttäuscht (z. B. E-Mails innerhalb eines Tages beantworten).
- ◆ Pfuscher am Anfang rächt sich

### 3.5.4 Electronic Commerce

Da alle Datenpäckchen, die durch die weite Welt reisen, von jedermann abgehört werden können, ist die Weitergabe von beispielsweise Kreditkartendaten nicht zu empfehlen. Wobei auch hier manchmal übertrieben wird, auch ein Kellner kann mit Ihrer Kreditkarte ein paar Blankobelege herstellen und er hat sogar ein Unterschriftsmuster zum Nachmachen.

Bis Ende 2000 gibt es in Deutschland mehr als 20000 Unternehmen mit Standleitungsanschluß ans Internet. Bei allen Formen des E-Commerce kommt der sicheren Datenübertragung im Netz eine besondere Bedeutung zu.

Unter "Electronic Commerce" versteht man Handel und Dienstleistungen aller Art über das Internet. Unterschieden werden dabei unter anderem folgende Bereiche:

## INTERNET - Möglichkeiten und Dienste

### ◆ *Electronic Banking*

Im Juni 1998 wurden 3.5 Millionen von insgesamt 80 Millionen Girokonten in Deutschland online verwaltet, davon 93% bei T-Online. Verwendete Sicherungstechniken:

- ◇ Geschlossenes Netz: T-Online ist ein Online-Dienst mit eigenem Angebot (Mailboxsystem). Die Daten gehen nicht ins allgemeine Internet. Homebanking erfolgt mit einer eigenen Bedienoberfläche.
- ◇ HBCI 2.0: Java-Anwendung, integriert in die Verfahren der Deutschen Bank, der Bank 24, der Landesgirokasse Stuttgart u.a.
- ◇ Verschlüsselung: Die Hypovereinsbank hat eine offizielle Ausfuhrgenehmigung der US Regierung für eine 128-Bit-Verschlüsselung, realisiert mit ActiveX Controls.
- ◇ Spezialsysteme, in der Regel Eigenentwicklungen: z.B. SafePassage-Proxy bei der Commerzbank oder eine Sammlung zertifizierter Active-X Skripten bei der HypoVereinsbank.

Gemeinsam sind fast allen Verfahren die Verwendung von PIN (Personal Identification Number) und TAN (Transaction Number), ansonsten sind sie nicht kompatibel. Lösungen, die umfangreiche Softwarekomponenten auf den Heimrechner transportieren, setzen entsprechend lange Login-Zeiten voraus. Oft genügt ein einmaliger Download der entsprechenden Software. Eine Transaktion kann schlimmstensfalls teurer werden als bei der herkömmlichen Bank um die Ecke.

### ◆ *Electronic Cash*

Hier existieren verschiedene nicht miteinander kompatible Verfahren, z. B. Cybercash oder E-Cash. Die "anonyme" Buchung von Bargeld auf einer Chipkarte fällt nicht unter den Begriff E-Cash.

### ◆ *Business-to-Consumer B2C*

Unter B2C versteht man alle E-Commerce-Beziehungen zwischen kommerziellen Anbietern und Endbenutzern. Typische Bereiche, in welchen sich für Endbenutzer signifikante Vorteile gegenüber traditionellen Handelsformen ergeben, sind die Auswahl und der Verkauf von

- ◇ Tickets und Reservierungen,
- ◇ Modeartikeln (z. B. Kleidung, Schuhe, Accessoires),
- ◇ Telekommunikationsgeräten,
- ◇ Geschenkartikeln im weitesten Sinne.

Bei *Internet-Auktionen* werden via WWW von beliebigen Endbenutzern die Daten eines zu verkaufenden Gegenstandes (oder einer Dienstleistung) auf einer Web-Seite eingetragen. Der betreffende Web-Server wird als kommerzielle Seite von einem Internet-Auktionshaus bereitgestellt.

Beim *Power Shopping* werden im WWW die Kaufwünsche von vielen Endbenutzern gesammelt und dann zur Erzielung eines niedrigeren Preises gebündelt an den Anbieter eines Produktes geleitet.

Die *Internet-Marktforschung* ist derzeit ein schnell wachsendes Anwendungsgebiet mit hohem Potential. Vergleiche aus der Medienbranche zeigen, daß dabei die Umfrage per Internet Resultate ergibt, die nahezu identisch denen einer klassischen Befragung sind.

Neben der Abwicklung von einfachen Bankgeschäften (Internet-Banking, s. o.) ist der *Wertpapierhandel* über das Internet von Bedeutung, der von Banken ebenso wie von spezialisierten Discount-Brokern angeboten wird.

### ◆ *Business-to-Business B2B*

Unter B2B versteht man alle E-Commerce-Beziehungen zwischen kommerziellen Anbietern und Nutzern ohne Einbeziehung von Endverbrauchern.

*Electronic Data Interchange EDI* ist die Sammelbezeichnung für den Datenaustausch zwischen den EDV-Anlagen von Unternehmen. Bei der *elektronischen Beschaffung*

## INTERNET - Möglichkeiten und Dienste

(*E-Procurement*) handelt es sich um die Internet-basierte Beschaffung von Waren aller Art für die Zwecke von Firmen. Dabei können bis zu 80% des Beschaffungsaufwandes eingespart werden.

*Application Service Provider* sind Firmen, die bestimmte EDV-Anwendungen im Internet professionellen Kunden zur Verfügung stellen, welche diese sonst aus Kosten- oder anderen Gründen nicht realisieren würden. Auf diese Weise können z. B. kleine und mittlere Unternehmen CAD-Systeme nach dem Stand der Technik benutzen. *Mitarbeiterschulung im Intranet (Teleteaching)* ist in Firmen ein wachsender Bereich, da hiermit die Organisationskosten der Schulung drastisch reduziert werden können.


### 3.6 Die eigene Homepage


Erfreulich ist, daß nicht nur Firmen, sondern auch jeder Privatmann sein Image mit einem WWW-Server pflegen kann. Teuer ist so etwas nur, wenn man gleich seine eigene Domain (wie z. B. 'microsoft.com' oder 'netzmafia.de') haben möchte.

Ob sich die Präsentation der eigenen Person oder vielleicht des eigenen Hobbys mit den Präsentationen großer Firmen messen kann, hängt von der Phantasie und den Fähigkeiten des einzelnen ab. Für die ersten Schritte ist es sowieso günstiger, sich unter die Fittiche eines Providers zu begeben. Da ein WWW-Server rund um die Uhr im Netz verfügbar sein muß, sind auch die Anfangsinvestitionen (Rechner, Netzanbindung etc.) und auch die monatlichen Belastungen für eine Standleitung recht hoch. Die meisten Provider bieten einen Platz auf ihrem WWW-Server zu einer Monatspauschale an. Man muß sich nicht um die Rechnertechnik kümmern und kann sich voll auf die Gestaltung des Angebots konzentrieren. So beschränkt sich die Investition auf den Modem- oder ISDN-Zugang zum Provider, da man sich ja nur zur Datenpflege einloggen muß. Die Provider können in der Regel auch die Domain handhaben (der Fachbegriff dafür ist 'Multihoming' oder 'virtual host'). Wer speziellere Dinge vorhat, beispielsweise Datenbankabfragen über WWW, kann bei den meisten Providern ein eigenes Rechnersystem aufstellen und spart so zumindest die Standleitungskosten.

Für Sie stellt sich die Frage, wie Sie Ihr Unternehmen am besten präsentieren. Zunächst werden Sie potentielle Kunden mit einem sauber aufbereiteten Angebot locken. Dazu gehört eine ansprechende Gestaltung der WWW-Seiten mit einer einheitlichen Linie - ein roter Faden, der sich in Erscheinungsbild und Benutzerführung durch das gesamte Angebot zieht. Statt mit einem Riesenmenü zu beginnen und dann nach dem ersten Link nur ein Baustellenschild zu zeigen ('Diese Seite befindet sich noch im Aufbau'), läßt man besser die Menüpunkte weg, bis man handfeste Informationen bieten kann. Damit interessierte Web-Surfer nicht gleich wieder verschwinden, muß das Informationsangebot möglichst vielfältig und aktuell sein.



 [Zum Inhaltsverzeichnis](#)

 [Zum nächsten Abschnitt](#)

---

Copyright © Prof. Jürgen Plate, Fachhochschule München



## INTERNET - Möglichkeiten und Dienste

*Prof. Jürgen Plate*

---

# 4 Kriminalität und Sicherheit im Internet

*"Within any community of 20 million people,  
there's bound to be a red-light district."*

*Brian Behlendorf*

Einleitend möchte ich ein paar grundsätzliche Dinge klarstellen und danach auf einige juristische und sicherheitstechnische Aspekte eingehen.

Der WDR tut es, ZAK tut es, c't hat es getan, Und EMMA tut es immer wieder: Berichte über Sex im Internet bringen. Warum sie das tun, ist klar. Es ist eines der heißesten Themen der deutschen Presse, Menschen regen sich auf, Emotionen schlagen hoch - oder lassen sich zumindest damit hochschlagen. Kurz gesagt: Berichte über Sex mitten auf der Datenautobahn sind in. Und wenn es nicht um Sex geht, dann liest man, daß jugendliche Terroristen die Bauanleitungen für Bomben aus dem Internet holen. Außer dem ist das Netz Tummelplatz für Rechts-, Links- oder Sonstwas-Extremisten.

Da sich jedoch auch seriöse Magazine wie Zeit, Spiegel oder FAZ auf dieses Thema gestürzt haben, ist eine kurze Bemerkung dazu nötig. Zunächst eine pauschale Antwort: Es stimmt; im Internet gibt es Sex und all das andere. Nun müssen wir das Ganze aber relativieren: Das Internet spiegelt unsere menschliche Gesellschaft wieder - also kommen auch Sex und politische Randgruppen vor.

Auch die Bombenbauanleitungen sind im Netz zu finden, denn schließlich hat man Zugang zu Informationsservern auf der ganzen Welt. Ein paar Anleitungen, die durch die News geisterten (rec.pyrotechnics), habe ich gelesen. Sie sind gefährlich - für den der sie ernst nimmt und versucht, sie nachzuvollziehen. Der Bastler riskiert Leib und Leben, denn die Texte sind fehlerhaft und von mangelndem Fachwissen geprägt. Auch für derartige Informationen braucht man das Netz nicht, ein paar gute Chemie- und Physikbücher tun es auch - und die gibt es in jeder öffentlichen Bibliothek. Hier zeigt sich auch der Nachteil der offenen Struktur. Jeder, der sich berufen fühlt, kann erst einmal Informationen ins Netz streuen. Wenn sich dann Proteste erheben, ist es oft zu spät. Daraus folgt die Regel: "Sei mißtrauisch!"

Extremisten können das Netz für die Übermittlung von E-Mail oder Dateien nutzen - auf dieselbe Art und Weise, wie sie Telefon, Brief- und Paketpost nutzen können. Und genausowenig wie die Post für die Verabredung einer Straftat am Telefon ist, kann das Netz etwas dafür, wenn es auf diese Weise mißbraucht wird. Server mit Nazi-Material in den USA unterliegen dort dem Gesetz zum Schutz der freien Rede und sind daher schwer angreifbar.

Grundsätzlich gilt, wie schon gesagt, daß sich alle Dinge des täglichen Lebens und alle Facetten der Gesellschaft im Netz wiederspiegeln - und das sind nun mal nicht immer nur positive Dinge.

## 4.1 Juristisches

Das Internet ist eine gewachsene Struktur, die sich von keiner übergreifenden Ordnung beherrschen läßt. Es bietet jedem Raum für seine Kreativität, egal ob er kommerzielle Interessen verfolgt oder nur seinem Hobby frönen möchte. Ein Problem bleibt jedoch bestehen: Das Internet verbindet viele Länder mit unterschiedlicher Gesetzgebung, die auch die Aktivitäten im Netz tangieren. So ist beispielsweise das Versenden von verschlüsselter E-Mail nach Frankreich nicht erlaubt. Wer jedoch alle Gesetze der Welt auf das Internet anwenden will, wird damit letztlich scheitern.

In Deutschland wird das Internet von etlichen Paragraphen berührt:

### **Strafgesetzbuch:**

- Unbefugte Datenbeschaffung
- Unbefugtes Eindringen in ein Datenverarbeitungssystem
- Datenbeschädigung

## **Gesetz zur Bekämpfung der Computerkriminalität:**

- *Ausspähen von Daten*

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

(1) Wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft,
- *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. Daten verändert (s. o.) oder
  2. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt oder unbrauchbar macht, beseitigt oder verändert,

wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

## **Bundesgesetz über den Datenschutz**

Die folgenden Ausdrücke bedeuten:

- **Personendaten (Daten):** alle Angaben, die sich auf eine bestimmte oder bestimmbar Person beziehen.
- **Betroffene Personen:** natürliche oder juristische Personen, über die Daten bearbeitet werden.
- **Besonders schützenswerte Personendaten:** Daten über
  1. Die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten.
  2. Die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit.
  3. Maßnahmen der sozialen Hilfe.
  4. Administrative oder strafrechtliche Verfolgungen und Sanktionen.
- **Persönlichkeitsprofil:** eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.
- **Bearbeiten:** jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten
- **Bekanntgeben:** das Zugänglichmachen von Personendaten wie das Einsichtgewähren, Weitergeben oder Veröffentlichen
- **Datensammlung:** jeder Bestand von Personendaten, der so aufgebaut ist, daß die Daten nach betroffenen Personen erschließbar sind
- **Bundesorgane:** Behörden und Dienststellen des Bundes sowie Personen, soweit sie mit öffentlichen Aufgaben des Bundes betraut sind
- **Inhaber der Datensammlung:** private Personen oder Bundesorgane, die über den Zweck und Inhalt einer Datensammlung entscheiden
- **Grundsätze**
  1. Personendaten dürfen nur rechtmäßig beschafft werden.
  2. Ihre Bearbeitung hat nach Treu und Glauben zu erfolgen und muß verhältnismäßig sein.

3. Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.

### 4.2 Copyright-Probleme

Wie bei Zeitungen, Büchern, Radio- und Fernsehsendungen oder anderen Formane der Publikationen unterliegen auch alle Veröffentlichungen im Internet dem Copyright. Doch in der Regel publizieren die Internet-Teilnehmer nicht, um Geld zu verdienen, sondern aus freien Stücken. Sie kämen auch nie auf den Gedanken, ihre Mitmenschen mit Copyright-Prozessen zu überziehen - im Gegenteil, sie freuen sich, wenn ihre Ideen übernommen werden. Ohnehin bleibt fraglich, ob sich der klassische Copyright-Begriff auf die Welt des Internet übertragen läßt. Es herrscht allgemeine Übereinkunft darüber, daß sich Ideen nicht durch Copyright schützen lassen. Wäre es anders, müßten praktisch alle kommerziellen Softwareprodukte eingestampft werden, weil sie schließlich zu einem Großteil auf Algorithmen beruhen, die unter anderem auch im Netz veröffentlicht wurden. Da alle Quellen maschinenlesbar vorliegen, leicht zu kopieren und zu manipulieren sind, kann es unter Umständen sehr schwierig bis unmöglich sein, den wahren Urheber eines bestimmten Inhalts auszumachen. In Deutschland geht das Urheberrecht sogar noch weiter, man kann niemals die Urheberschaft an eine Schriftstück aufgeben, sondern lediglich das Nutzungsrecht.

### 4.3 Sicherheit

#### Allgemeines

Jeder, der seinen Rechner an das Internet anschließt, sich eine Internet-Adresse sowie die TCP/IP-Software besorgt und installiert, muß sich darüber im klaren sein, daß er damit seinen Rechner potentiell mit einigen Millionen anderer Rechner in Verbindung bringt. So wie man selbst alle möglichen fremden Rechner erreichen kann, ist man auch für jedermann kontaktierbar. Mit zunehmender Vernetzung wächst aber auch der Bedarf am Schutz der Privatsphäre. Während für die Briefpost und für die Telekom ein Postgeheimnis gilt, gibt es bei Mailboxen und Weitverkehrsnetzen nichts Vergleichbares. Bei einer Ansammlung von weltweit miteinander vernetzten Computern ist ein Briefgeheimnis auch nicht möglich. Nachrichten, die Sie beispielsweise über das Internet verschicken, laufen über viele Rechner (meist sind es aber nur Router). Theoretisch ist es an jeder Stelle im Netz möglich, Ihre Daten abzuhören und zu speichern. Zudem könnte jemand Dokumente unter Ihrem Namen übers Netz verschicken oder abgefangene Dokumente verfälschen (letzteres gab es natürlich seit der Antike auch schon beim Versand von Papierdokumenten und in neuerer Zeit bei Fernschreiben oder Telefax). Das Internet ist offen und um den Individualismus auf dem Netz so wenig wie möglich einzuschränken, müssen Sicherheitsvorkehrungen an den Endgeräten vorgenommen werden.

Für Nutzer von Unix- oder Windows-NT-Maschinen, bei denen in der Regel Server-Prozesse automatisch im Hintergrund laufen, heißt dies, daß sie ihre Maschinen gegen unberechtigten Gebrauch zu schützen haben. Sicherheitsempfindliche Netze können durch sogenannte Firewall-Systeme nach außen geschützt werden. Ein Firewall ist ein Rechner mit zwei Netzwerk-Schnittstellen. Auf der einen Seite wird die Verbindung zur großen, weiten Welt hergestellt, auf der anderen Seite werden die internen Rechner angeschlossen. Von außerhalb ist nur der Firewall-Rechner zu sehen; die interne Netzstruktur bleibt verborgen. Weiterer Vorteil: Es gibt nur eine einzige Schnittstellen nach außen, die sich gut überwachen läßt. Weiterhin werden alle Datenpakete zwischen den beiden Netzwerk-Schnittstellen vom Firewall weitergereicht. Man kann nun beispielsweise bestimmte Daten sperren. Es gibt dabei grundsätzlich zwei Strategien. Die erste Strategie verbietet gezielt bestimmte Dienste, z. B. Telnet-Logins, erlaubt aber alles andere - ein relativ offener Ansatz. Bei der zweiten Strategie wird alles verboten, was nicht explizit erlaubt ist.

Für bestimmte Dienste wurden oder werden Sicherheitsmaßnahmen getroffen. So wird auf Unix-Servern für WWW oder FTP für den Abfragenden das Datenverzeichnis zum

Wurzelverzeichnis. Auf diese Weise ist auch bei Sicherheitsmängeln im Serverprogramm niemals ein Zugriff auf Dateien außerhalb des reservierten Plattenbereichs möglich. Diese Methode kann man auch für den Betrieb einer Mailbox oder einen Gast-Login ohne Paßwort verwenden.

### **Sicherheit von Betriebssystemen**

In der Betriebssystemsoftware (und auch der Anwendungssoftware) treten immer wieder Fehler auf, die unautorisierten Zugang für Hacker durch Ausnutzen von Sicherheitslöchern zuläßt. Bei der Wahl eines Serverbetriebssystems sollten daher Sicherheitsaspekte im Vordergrund stehen und nicht die (scheinbar) leichte Bedienbarkeit. So haben beispielsweise Viren bei DOS- oder Windowsrechnern leichtes Spiel, weil sie alle Programme auf der Platte befallen können. Bei Systemen mit Zugriffsrechten für Dateien (Unix, Novell Netware, etc.) können sie meist nur die Programme eines Benutzers verseuchen. Je nach System gibt es unterschiedliche Methoden ein System zu manipulieren:

- Trojanische Pferde sind Programme, die einerseits die gewünschte bzw. "offizielle" Funktion ausführen, aber gleichzeitig vom Manipulateur beabsichtigte Nebenwirkung ausführen.
- Würmer oder Wurmsegmente sind Programme, die sich selbständig über ein Netz verbreiten und auf anderen Rechnern vervielfältigen können.
- Viren sind Programme, die sich in andere Programme hineinkopieren (reproduzieren) und zeit- oder ereignisgesteuert Schäden hervorrufen.
- Logische Bomben sind zusätzliche Programmfunktionen, die vom Programmierer eingebaut werden. Sie treten erst zu einem bestimmten Ereignis zu Tage, z. B. werden alle Daten zwei Jahre nach Entlassung des Programmierers gelöscht.
- Trap doors sind Programmfunktionen, die einen nicht autorisierten Zugang zum System ermöglichen. Dies muß nicht in böser Absicht geschehen, auch Programmteile, die zur Fehlersuche dienen und dann in der Verkaufsversion nicht entfernt wurden, oder Wartungaccounts können zu trap doors werden.
- In Netzen gibt es dann noch Formen der Tarnung (z. B. spoofing), bei der ein Rechner vorspiegelt, ein anderer zu sein. In vielen Betriebssystemen gibt es den Begriff des "trusted host". Vereinfacht gesagt sind dies Rechner, denen gegenüber der eigene Rechner "offen" ist. Tarnt sich ein fremder Rechner als vertrauenswürdiger Host, wird das Eindringen erleichtert.

Bis auf wenige Ausnahmen (z. B. ftp-Server, WWW-Server) sind bei PCs unter DOS, Windows 3.1x oder OS/2 keine Maßnahmen zur Sicherheit notwendig, da an PCs in der Regel keine Anwendungen gestartet sind, die Kontaktaufnahme von außen akzeptieren. Problematischer ist es schon bei Windows 95/98, oder den Macs von Apple, da hier prinzipiell ein Zugriff von außen möglich ist. Das ändert sich natürlich sofort, wenn Zugriffsdienst angeboten werden, z. B. der Zugriff auf die Platte über NFS oder auch Fax-, Modem- oder Druckerserver. Aber auch, falls kein solcher Dienst läuft, besteht die Möglichkeit sogenannter "denial of Service"-Attacken von einem fernen Rechner, die zumindest die Internet-Verbindung unterbrechen können.

Eine hardwareunabhängige Sammlung dieser Fehler und die Initiative zur Behebung derselben unternehmen die CERTs (Computer Emergency Response Team). Wie viele Einrichtungen im Internet existieren CERTs auf mehreren Ebenen. Das deutsche CERT (DFN-CERT) ist an der Uni Hamburg lokalisiert. Die gesammelten Informationen des CERT werden auf einem FTP-Server zur Verfügung gestellt. ([www.cert.dfn.de](http://www.cert.dfn.de)).

### **Abhören**

Da die Datenpakete ihren Weg mitunter über mehr als 20 Rechner nehmen können, besteht grundsätzlich die Möglichkeit, daß irgend jemand die Daten "abhört" (z. B. mit dem Programm "tcpdump") oder verändert weitergibt. Da auch die Paßworte beim Telnet- oder FTP-Login im Klartext weitergegeben werden, besteht die (normalerweise sehr geringe) Möglichkeit, daß jemand an diese Information kommt. Ebenso ist es dem Fachmann möglich, Absenderadressen bei News oder

## INTERNET - Möglichkeiten und Dienste

E-Mail zu fälschen ("fakemail", "fakenews", siehe oben). Es ist daher nicht ratsam, z. B. Kreditkartennummern oder andere vertrauliche Daten offen über das Internet zu versenden. Abhilfe schaffen hier beispielsweise kryptographische Verfahren und Methoden, eine Nachricht zu authentifizieren (elektronische Unterschrift).

Das Secure Socket Layer Protocol (SSL) verschlüsselt die Übertragung unterhalb der Ebene 3 des ISO/OSI 7-Schichten-Modells mit 40 Bit bzw. 128 Bit. Dazu müssen die beiden an der Übertragung beteiligten Hosts von einer übergeordneten Instanz autorisiert worden sein.

Darauf setzt das "Secure Hypertext Transfer Protocol" (https) auf: Zertifikate werden zwischen Client (WWW-Browser) und Server (WWW-Server) ausgetauscht, über die die beiden Beteiligten eindeutig identifiziert werden können. Netscape ab Version 2 und der MS Internet Explorer ab Version 3 verarbeiten das https-Protokoll. Bei Netscape wandelt sich im Fall einer sicheren Übertragung das

Symbol  zu .

### Social Engineering

Die größte Sicherheitslücke ist jedoch nach wie vor der Benutzer selbst. Paßwörter werden aufgeschrieben (klassisches Beispiel: der Zettel, der unter der Tastatur klebt) oder sie sind aus dem persönlichen Umfeld entnommen (Vornamen von Frau, Mann, Kindern, Hund, die eigene Telefonnummer, die Automarke usw.). Selbst das Paßwort "geheim" wird immer noch angetroffen. Auch "Joshua" aus dem Film "War Games" war eine Zeit sehr beliebt. Übertroffen wird das nur noch von "1234567" oder "qwertz". Wer sich ein kompliziertes Paßwort nicht merken kann, sollte zumindest ein paar Sonderzeichen einfügen oder das "l" durch die Ziffer "1" und das "o" durch die Ziffer "0" ersetzen. Man kann es auch mit den Anfangsbuchstaben eines Merksatzes versuchen. So ergibt z. B. "Fest gemauert in der Erden steht die Form aus Lehm gebrannt" (Schiller: Lied der Glocke) das Paßwort "FgidEsdFaLg". Es gibt übrigens Paßwort-Knackprogramme, die einfach und brutal das Rechtschreibwörterbuch, Namenslisten usw. verwenden, um Paßwörter durch Probieren herauszufinden.

### Schadensformen

- Hat eine nicht autorisierte Person Zugang zum Rechner erlangt, kann sie vertrauliche Daten stehlen oder sogar ändern. Durch Zurücklassen von Viren, Trojanischen Pferden oder Programmen mit logischen Bomben kann der Eindringling Sabotage verüben. Möglicherweise läßt er aber nur eine trap door zurück und begnügt sich mit der Inanspruchnahme von Plattenplatz und Rechnerleistung. Auch das kann unangenehm werden, wenn jemand Ihren WWW-Server als Depot für Pornobilder verwendet. Aber auch ohne in den Server einzudringen, kann jemand Ihnen im Internet Schäden zufügen.
- Gefälschte E-Mail (z. B. bei Bestellungen). Sowohl die Informationen im Kopf der E-Mail-Nachricht als auch der eigentliche Text werden im Klartext vom Sender zum Empfänger transportiert. Jeder mit ausreichenden Zugriffsrechten auf einem Durchgangssystem könnte die Post mitlesen oder verfälschen. Die einzige befriedigende Lösung besteht darin, zumindest den Text zu chiffrieren. Ein anderes Problem der Sicherheit von E-Mail besteht in der Möglichkeit, einen Brief zu fälschen. Da in der Regel das "From:"-Feld Aufschluß über den Absender gibt, kann nur die Abschätzung der Wahrscheinlichkeit helfen zu beurteilen, ob ein Brief von "president@whitehouse.gov" tatsächlich vom amerikanischen Präsidenten stammt.
- Gefälschte Newsbeiträge. Auf die gleiche Art und Weise kann sich jemand in den Newsgruppen, den schwarzen Brettern des Internet (genauer des USENET), als Angehöriger Ihres Unternehmens ausgeben und durch entsprechende Veröffentlichungen den Ruf der Firma empfindlich schädigen.

### Pretty Good Privacy

Schon seit längerer Zeit überlegen sich Experten, wie man die Sicherheitsprobleme in den Griff bekommen kann. Den interessantesten Ansatz, der auch schon rege benutzt wird, stellt ein mathematisches Verfahren dar, das auf Primzahlen basiert. Entwickelt wurde dieses Verfahren von den Amerikanern Rivest, Shamir und Adleman, die auch ein Patent auf einen entsprechenden Algorithmus haben (RSA-Algorithmus). Philip Zimmermann vom MIT hatte dieses Verfahren mit anderen kryptographischen Methoden kombiniert. Herausgekommen ist das leicht zu bedienende Freeware-Programm "pretty good privacy" (PGP), das inzwischen weltweit verbreitet ist und überall einen hervorragenden Ruf genießt.

Es gibt bei dem Verfahren zwei Schlüssel: einen öffentlichen und einen privaten. Zum Verschlüsseln einer Nachricht benutzt PGP den öffentlichen Schlüssel des Empfängers. Die verschlüsselte Datei kann nun auch über abhörbare Kanäle verschickt werden, denn nur der Besitzer des zu dem öffentlichen Schlüssel gehörenden privaten Schlüssels kann die chiffrierte Nachricht entschlüsseln. Selbst mit dem öffentlichen Schlüssel, der zum Chiffrieren benutzt wurde, läßt sich der Inhalt der Nachricht nicht mehr lesbar machen. Natürlich kann man jede Art von Dateien verschlüsseln. Auf Wunsch kann PGP die Datei automatisch noch komprimieren oder als 7-Bit-ASCII-Code ausgeben.

PGP kann aber noch mehr: Sie können nämlich ein Dokument mit einer Signatur versehen. PGP berechnet mittels kryptographischer Verfahren eine Art Quersumme über Ihr Dokument und verschlüsselt diese mit Ihrem privaten Schlüssel. Jeder Empfänger dieses Dokumentes kann nun mittels PGP und Ihrem öffentlichen Schlüssel die Signatur überprüfen. Wurde das Dokument unterwegs auch nur um ein Zeichen geändert, so wird dies von PGP erkannt und Ihnen mitgeteilt. Sehr nützlich ist auch die Möglichkeit, Verschlüsselung und Signatur zu kombinieren. Durch die Verschlüsselung gehen Sie sicher, daß nur der Adressat das Dokument lesen kann und durch die Signatur kann Ihr Adressat sicher gehen, daß dieses Dokument auch wirklich von Ihnen stammt.

Natürlich gibt es kein absolut sicheres kryptographisches Verfahren. Auch das von PGP benutzte Verfahren hat Sicherheitsrisiken. Da wäre zum einen die Verwaltung der Schlüssel. Selbstverständlich ist, daß Sie keinem anderen Menschen den Zugang zu Ihrem privaten Schlüssel erlauben. PGP speichert diesen in einer Datei, die durch ein von Ihnen gewähltes Paßwort geschützt wird. Sollte jemand nun in den Besitz dieser Datei und Ihres Paßwortes gelangen, so kann er alle Ihre Dateien entschlüsseln und Ihre elektronische Signatur benutzen.

Ein weiterer Angriffspunkt ist die Verbreitung des öffentlichen Schlüssels. PGP kann Ihren öffentlichen Schlüssel in einer Datei speichern, die Sie dann an Ihre Freunde weitergeben oder im Internet veröffentlichen können. Was aber, wenn ein Fremder einen öffentlichen Schlüssel unter Ihrem Namen veröffentlicht? Eine mit diesem Schlüssel chiffrierte Nachricht kann dann nur von dem Fremden gelesen werden und nicht von Ihnen. Am besten wäre es, wenn es eine vertrauenswürdige Institution gäbe, die eine Art Telefonbuch der öffentlichen Schlüssel führen würde. Leider wird es diese Institution auf absehbare Zeit nicht geben. Also müssen Sie sicherstellen, daß ein von Ihnen benutzter öffentlicher Schlüssel auch wirklich der gewünschten Person gehört.

PGP gibt es für DOS, Macintosh und Unix (für fast alle Versionen). Natürlich sind die Formate kompatibel, d. h. eine auf einem Mac verschlüsselte Nachricht kann auch auf einem DOS-System gelesen werden. Für graphische Oberflächen gibt es meist schon Shells, die die Benutzung von PGP vereinfachen.

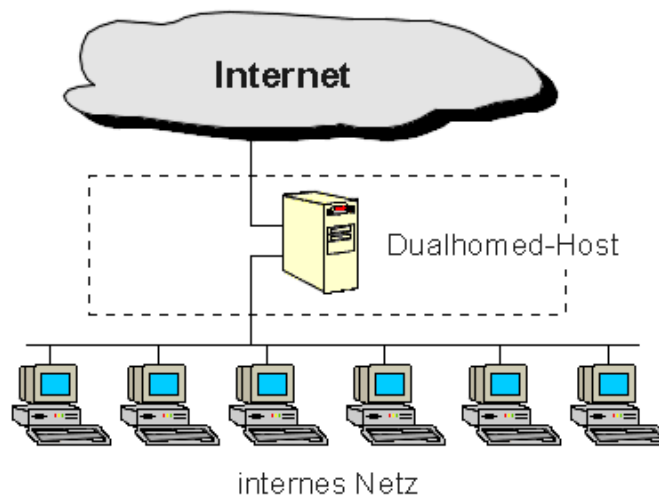
Kostenlose Versionen und Versionen mit erweitertem Umfang gibt es unter <http://www.pgp.com> bzw. <http://www.pgpinternational.com>.

## 4.4 Schutz des Netzwerks durch Firewalls

Für Nutzer von Unix- oder Windows-NT-Maschinen, bei denen in der Regel Server-Prozesse automatisch im Hintergrund laufen, heißt dies, daß sie ihre Maschinen gegen unberechtigten Gebrauch zu schützen haben. Sicherheitsempfindliche Netze können durch sogenannte Firewall-Systeme nach außen geschützt werden. Ähnlich der Zugbrücke einer Burg erlauben sie den Zugang nur an einer definierten Stelle. Damit läßt sich der Datenverkehr von und nach außen kontrollieren. Normalerweise sind zahlreiche Rechner des Unternehmens, die unter diversen Betriebssystemen laufen, direkt aus dem öffentlichen Netz erreichbar. Ein Firewall kanalisiert die Kommunikation, indem alle Daten von und nach außen über dieses System laufen müssen. Die Kanalisierung erhöht zudem die Chancen, einen Einbruchversuch anhand ausführlicher Protokoll-Dateien zu erkennen, da der Eindringling erst den Firewall passieren muß. Mit einem Firewall läßt sich die Wahrscheinlichkeit erheblich verringern, daß Angreifer von außen in inneren Systeme und Netze eindringen können. Zudem kann das System interne Benutzer davon abhalten, sicherheitsrelevante Informationen, wie unverschlüsselte Paßwörter oder vertrauliche Daten, nach außen geben. Ein Firewall kann aus einer einzelnen Maschine oder aus einer mehrstufigen Anordnung bestehen. Eine mehrstufige Anordnung ist vor allem dann sinnvoll, wenn man bestimmte Dienste der Öffentlichkeit zur Verfügung stellen will, etwa einen WWW- oder ftp-Server. Die entsprechenden Hosts können dann in einem Zwischennetz isoliert werden. Nachfolgend sollen einige gängige Firewall-Architekturen vorgestellt werden.

### 4.4.1 Architektur mit Dualhomed-Host

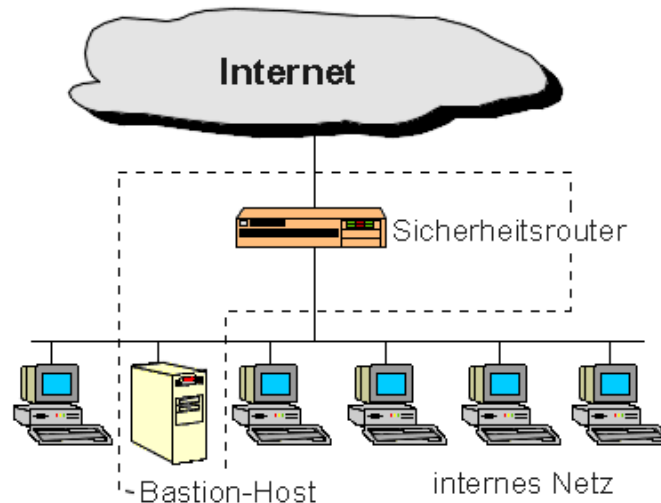
Eine Architektur mit Dualhomed-Host wird um einen Rechner herum aufgebaut, der über mindestens zwei Netzwerkschnittstellen verfügt. Ein solcher Host ist als Router zwischen den Netzen einsetzbar, die an die Schnittstellen angeschlossen sind. Er kann dann IP-Pakete von Netz zu Netz routen. Für diese Firewall-Architektur muß diese Routingfunktion jedoch deaktiviert werden.



IP-Pakete werden somit nicht direkt von dem einen Netz (dem Internet) in das andere Netz (das interne, geschützte Netz) geroutet. Systeme innerhalb der Firewall und Systeme außerhalb (im Internet) können jeweils mit dem Dualhomed-Host, aber nicht direkt miteinander kommunizieren. Der IP-Verkehr zwischen ihnen wird vollständig blockiert. Die Netzarchitektur für eine Firewall mit Dualhomed-Host ist denkbar einfach: der Dualhomed-Host sitzt in der Mitte, wobei er mit dem Internet und dem internen Netz verbunden ist. Ein Dualhomed-Host kann Dienste nur anbieten, indem er entsprechende Proxies (Stellvertreter) oder Gateways einsetzt. Es ist jedoch auch möglich, direkte Nutzerzugriffe zu gestatten (Sicherheitsrisiko).

### 4.4.2 Architektur mit überwachtem Host

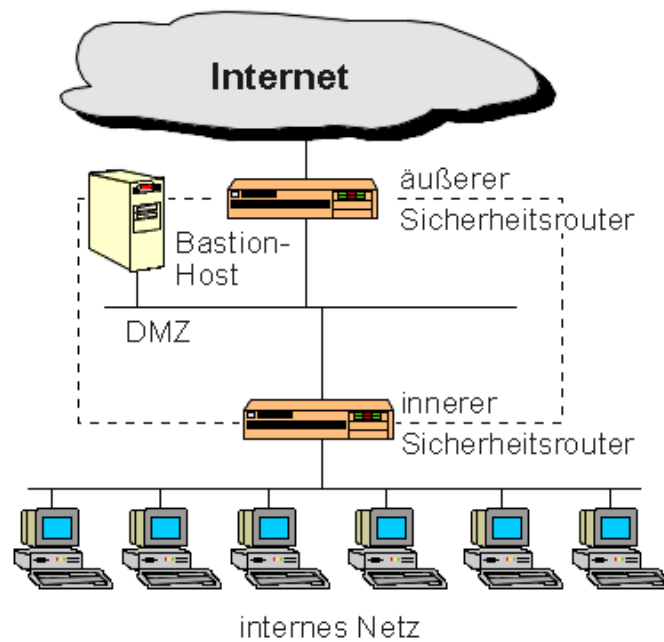
Die "screened host architecture" bietet Dienste von einem Rechner an, der nur an das interne Netz direkt angeschlossen ist, wobei ein getrennter Router verwendet wird. Der Bastion-Host befindet sich im inneren Netz. Auf diesem Router verhindern Paketfilter das Umgehen des Bastion-Host. Die Paketfilterung auf dem Sicherheitsrouter muß so konfiguriert werden, daß der Bastion-Host das einzige System im internen Netz darstellt, zu dem Rechner aus dem Internet Verbindungen aufbauen können (das einzige "nach außen sichtbare" System). Zusätzlich sind nur gewisse Dienste zugelassen.



Alle externen Systeme, die auf interne Systeme zugreifen wollen, und auch alle internen Systeme, die externe Dienste wahrnehmen wollen, müssen sich mit diesem Rechner verbinden. Daraus ergibt sich ein besonderes Schutzbedürfnis für diesen Bastion-Host. Der Vorteil bei dieser Konstruktion ist die Tatsache, daß ein Router leichter zu verteidigen ist. Dies liegt u. a. daran, daß auf ihm keine Dienste angeboten werden. Nachteilig wirkt sich aus, daß bei einer eventuellen Erstürmung des Bastion-Host das interne Netz vollkommen schutzlos ist.

### 4.4.3 Architektur mit überwachtem Teilnetz

Die "screened subnet architecture" erweitert die Architektur mit überwachtem Host um eine Art Pufferzone, die als Grenznetz das interne Netz vom Internet isoliert. Diese Isolierzone wird auch "Demilitarisierte Zone" (DMZ) genannt.



Bastion-Hosts sind von ihrer Art her die gefährdetsten Rechner in einer Firewallkonstruktion. Auch wenn sie in der Regel mit allen Mitteln geschützt sind, werden sie doch am häufigsten angegriffen. Die Ursache liegt darin, daß ein Bastion-Host als einziges System Kontakt zur Außenwelt unterhält.

### 4.4.4 Firewall-Software

Zur Software-Konfiguration eines Firewall existieren zwei Grundstrategien:

- "Es ist alles erlaubt, was nicht verboten ist". Dieser Ansatz schließt die Nutzung bestimmter Dienste (z. B. tftp, nfs) generell aus. Er ist benutzerfreundlich, da neue Dienste automatisch erlaubt sind, aber auch gefährlich, da der Administrator das Verhalten der Nutzer ständig beobachten und rechtzeitig Gegenmaßnahmen treffen muß.
- "Es ist alles verboten, was nicht erlaubt ist". Diese Strategie könnte von den Nutzern als hinderlich angesehen werden, da diese neue Dienste erst umständlich beantragen müssen. Sie schützt aber auch vor Sicherheitslücken im Betriebssystem und in Anwendungsprogrammen, da sie den Zugriff auf unbekannte Ports unterbindet.

In bezug auf die Schicht des OSI-Modells gibt es drei Arten von Firewall-Systemen:

- Paketfilter überprüfen die Quell- und Zieladresse (IP-Adresse und TCP/UDP-Port) eines Pakets und entscheiden, ob es passieren darf oder nicht. Der Vorteil besteht in der Transparenz für den Anwender. Diese Transparenz ist aber zugleich von Nachteil: Paketfilter können nicht zwischen Nutzern und deren Rechten unterscheiden. Paketfilter sind im allgemeinen auf Routern angesiedelt und werden heute von den meisten Herstellern mitgeliefert. Intelligente Paketfilter analysieren zusätzlich den Inhalt der Pakete und erkennen auch die Zulässigkeit von Verbindungen, die einfache Paketfilter nicht erlauben würden (z. B. Datenverbindung bei ftp).
- Circuit Level Gateways sind mit Paketfiltern vergleichbar, arbeiten jedoch auf einer anderen Ebene des Protokollstacks. Verbindungen durch solch ein Gateway erscheinen einer entfernten Maschine, als beständen sie mit dem Firewall-Host. Somit lassen sich Informationen über geschützte Netzwerke verbergen.

- Application Gateways, auch "Proxy" (Stellvertreter) genannt, stellen ein anderes Firewall-Konzept dar. Hierbei wird auf dem Firewall-Host für jede zulässige Anwendung ein eigenes Gateway-Programm installiert. Der Client muß sich dabei oftmals gegenüber dem Proxy-Programm authentifizieren. Dieser Proxy führt dann alle Aktionen im LAN stellvertretend für den Client aus. Damit lassen sich zum einen benutzerspezifische Zugangsprofile (welche Zeiten, welche Dienste, welche Rechner) erstellen, zum anderen kann man die Festlegung der zulässigen Verbindungen anwendungsbezogen vornehmen. Die daraus resultierenden separaten kleinen Regelsätze bleiben besser überschaubar als der komplexe Regelsatz eines Paketfilters. Application Gateways sind typische Vertreter der "Verboten-was-nicht-erlaubt"-Strategie und als die sicherste, aber auch aufwendigste Lösung einzuschätzen. Da beim Proxy alle Zugriffe nach außen über eine Instanz laufen, kann man den Proxy gleichzeitig als Cache (Pufferspeicher) benutzen. Der Proxy speichert alle erhaltenen WWW-Seiten zwischen, so daß er bei einem erneuten Zugriff darauf - egal, ob vom selben oder einem anderen Anwender - keine Verbindung nach außen aufbauen muß.

Der Einsatz von Firewalls bietet sich auch innerhalb einer Organisation an, um Bereiche unterschiedlicher Sensitivität von einander abzugrenzen. Firewalls bieten jedoch niemals hundertprozentige Sicherheit! Sie schützen nicht vor dem Fehlverhalten eines autorisierten Anwenders und können, etwa durch eine zusätzliche Modem-Verbindung, umgangen werden.

### 4.5 Obscure URLs

Web-Adressen lassen sich nicht nur in der bekannten Form als vier Zahlen zwischen 0 und 255 darstellen, die durch Punkte getrennt werden. Man kann sie auch als zehnstellige Dezimalzahl darstellen, z. B. **http://2368208338** für **www.netzmafia.de** (141.39.253.210). Eine IP-Adresse ist aus Rechnersicht ja eine 32-Bit-Dualzahl und die kann man dezimal darstellen. Wenn eine solche URL beispielsweise als Link auf einer Site oder in einer Mail auftaucht, hat der Anwender keinen Anhaltspunkt, welche Site er besucht. Es gibt noch weitere Möglichkeiten, Surfer darüber zu täuschen, auf welche Sites sie etwa der Versender einer Werbemail locken will. Die Methoden, URLs unkenntlich zu machen, beruhen meist auf der Darstellung einer IP-Adresse als 32-Bit-Dualzahl, kurz als "Dword". Der Begriff stammt von "Double Word", also zweimal 16 Bit. Aber wir packen noch ein paar Tricks hinzu.

Als Beispiel diene die URL **http://www.microsoft.de@2368208338**. Sie führt nicht zu Microsoft, sondern wieder zur Website von Netzmafia, obwohl ihr Aussehen etwas anderes vermuten lässt. Es sieht so aus, als ließen sich mit ein paar Sonderzeichen und Ziffern URLs beliebig fälschen. Es handelt sich dabei nur um Tricks, die überflüssigen Text wie Teile einer URL aussehen lassen, andererseits die URL selbst verbergen. Jedes "@" Zeichen in einer URL verrät, daß alles, was davor steht, nicht Teil dieser URL ist. Solche Adressbestandteile verwendet man sonst für eine individuelle Anmeldung an einer Website oder bei einem FTP-Server. Der Teil vor dem "@" enthält dann den Benutzernamen oder eine Kombination aus Benutzernamen und Passwort (getrennt durch einen Doppelpunkt). Auch wenn eine Web-Seite keinen Benutzernamen benötigt, darf man einen angeben. Hinter dem "@" steht dann die eigentliche URL. Diese ist hier im Beispiel als Dword-Zahlenkolonne maskiert, so daß der Trick nicht gleich erkannt wird.

Probieren wir nun einmal **http://www.microsoft.de%402368208338**. Auch hier landen Sie wieder bei der Netzmafia. Hier wurde der Trick verfeinert. Die URL entspricht genau der ersten, nur daß hier der "@" durch "%40" ersetzt wurde. Die "40" ist der hexadezimale Wert des Zeichens "@". Innerhalb einer URL lassen sich alle ASCII-Zeichen auch durch den entsprechenden Zahlenwert darstellen, wenn ein Prozentzeichen vorangestellt wird. Sie erreichen unsere Website daher auch durch die Eingabe von **http://www%20netzmafia%20ede**, weil "2e" der hexadezimale Ascii-Wert für einen Punkt ist.

## INTERNET - Möglichkeiten und Dienste

Wie bekommt man den Dword-Wert einer URL? Dazu brauchen Sie nur einen Taschenrechner oder auch den Rechner von Windows. Sie müssen jetzt nur noch den Wert der IP-Adresse ausrechnen. Am Beispiel Netzmafia (141.39.253.210) sieht die Eingabe an Rechner so aus:

**141** [\*] 256 [=][+] **39** [=][\*] 256 [=][+] **253** [=][\*] 256 [=][+] **210** [=]

[=], [\*] und [+] sind die entsprechenden Rechnertasten. Mathematisch notiert lautet die Umrechnung:

$(((((141 * 256) + 39) * 256) + 253) * 256) + 210$

Wenn Sie es nun noch weiter treiben wollen, können Sie auch noch Hexadezimalzahlen (Basis 16) verwenden - aber Vorsicht: Ältere Browser und die Netscape-Navigatoren können damit nichts anfangen. Die Netzmafia-Adresse wird dann zu **http://0x8D.0x27.0xFD.0xD2**. Damit der Browser erkennt, daß es sich um Hex-Zahlen und nicht Dezimalzahlen handelt, wird die Zeichenkette "0x" (Null und kleines "x") davorgesetzt.



[Zum Inhaltsverzeichnis](#)



[Zum nächsten Abschnitt](#)

---

Copyright © Prof. Jürgen Plate, Fachhochschule München



## INTERNET - Möglichkeiten und Dienste

*Prof. Jürgen Plate*

---

# 5 INTRANET - Internet im Kleinen

## Prolog



Oft hört man: 'Internet? Ist das nicht gefährlich? Sind dort nicht die Hacker, die in Computer einbrechen, Daten verändern oder Viren auf den PC kopieren? Sind da nicht die Anbieter von Software-Raubkopien und Pornos? Nee, lieber nicht!' Natürlich stimmt das in gewisser Weise, aber man kann sich schützen.

Ein anderer Faktor spielt aber auch eine gewichtige Rolle, die Kosten für den Internet-Zugang. Diese liegen für den reinen Nutzer relativ niedrig. Hier sind wohl die Telefonkosten des Einfach-Internet-Zugangs der größte Faktor. Anders sieht es bei einer Web-Präsenz mit WWW-Server und anderen Diensten aus. Hier liegen die monatlichen Kosten für die Anbindung alleine bei mindestens ca. 250 bis 300 Mark pro Monat. Für Konzept, Webdesign, etc. muß man ein Vielfaches rechnen.

Aber man kann die Technik und die Programme des Internet auch im lokalen Netz nutzen, denn ein **Intranet** ist ein Kommunikationsnetz, daß sich derselben Technik bedient wie das Internet - es beschränkt sich lediglich auf den lokalen Einsatz.

## 5.1 Inhouse-Kommunikation vereinfachen

Der Informationsfluß in vielen Unternehmen oder Organisationen leidet unter etlichen Kommunikations- und Darstellungsproblemen. Im Lauf der Jahre sind unterschiedliche Systeme eingeführt worden, die teilweise untereinander nicht kompatibel sind. Je nach Programm ist die Bedienung oft auch nicht leicht zu erlernen und falls doch, ist auf jeden Fall jedes Programm unterschiedlich in seiner Bedienung.

Auch die Kommunikationswege sind höchst unterschiedlich: Vom Zettelverteilsystem (Hausmitteilung, Rundschreiben) über das schwarze Brett bis hin zu E-Mail, Datenbankabfrage und Groupware. Es gibt

- heterogene Formate,
- Medienbrüche (Papier, Mikrofilm, digital, ...),
- Probleme beim Datenaustausch zwischen Abteilungen,
- langsamen Informationsfluß,
- kostenintensive Verteilung der Info,
- redundante Datenhaltung,
- und vieles mehr.

Mit Internet-Diensten wie E-Mail, News und WWW bietet sich die Möglichkeit, alle Informationen mit einem einzigen Programm, dem WWW-Browser darzustellen. Es ist also nur noch die Bedienung eines einzigen Programms zu erlernen. Die Informationsaufbereitung kann in Form von WWW-Seiten in der Beschreibungssprache HTML (HyperText Markup Language) erfolgen. Beim Einstieg ist an einigen Stellen sicher zusätzlicher Programmieraufwand für die Datenkonvertierung nötig, aber letztendlich ist es egal, ob das Ergebnis einer Datenbankabfrage für einen Drucker oder für einen WWW-Browser aufbereitet werden muß. Im einfachsten Fall genügen jeweils eine Zeile zu Beginn und am Ende eines Dokuments:

- `<html><head><title>Dokumententitel</title></head><body><pre>`
- Hier kommt dann der Text des Dokuments
- `</pre></body></html>`

## INTERNET - Möglichkeiten und Dienste

Zu einem 'echten' WWW-Dokument gehört natürlich mehr: Strukturierung des Textes, Einfügen von Querverweisen (das Minimum wäre eine hierarchische Menüstruktur), Einbinden von Bild- und Tondokumenten.

Wichtigste Anwendung ist aus meiner Sicht nach wie vor die elektronische Post, 'E-Mail' genannt. Im Gegensatz zum Telefon, wo beide Partner gleichzeitig anwesend sein müssen, hat man bei E-Mail eine zeitliche Entkopplung - der Partner ist insofern immer erreichbar. Außerdem lassen sich per E-Mail auch andere digital gespeicherte Informationen, z. B. Texte, Bilder, etc., verschicken. Im Gegensatz zum Fax, das auch eine zeitliche Entkopplung der Partner schafft, lassen sich bei E-Mail die Daten im Computer gleich weiterverarbeiten.

### 5.2 Web-Publishing und Data Warehousing

Man wird auch sicher zuerst nur neue Informationen 'Web-konform' aufbereiten und erst nach und nach die älteren Daten aufarbeiten (wobei hier gleich eine Aktualisierung erfolgen kann). So kann prinzipiell jeder in einem Unternehmen oder einer Organisation Informationsanbieter werden. Dabei werden zwei Konzepte unterschieden:

- Intra-Web-Publishing stellt den Benutzern im Netz WWW-Dokumente zur Verfügung. Dazu müssen die Dokumente im HTML-Format auf einen WWW-Server abgelegt werden. Da der Transportmechanismus für solche Dokumente im Netz recht einfach ist, kann ein Server auch mit recht bescheidenen Mitteln eingerichtet werden. Beispielsweise würde ein PC mit 16 MByte RAM und einem 486er-Prozessor schon ausreichen. Die Server-Software ist für viele Plattformen verfügbar, z. B. für Novell Netware, Windows 95/NT oder für UNIX. Der Vorteil der Datenaufbereitung im HTML-Format und die Tatsache, daß jeder Rechner im Netz, auf dem ein Browser installiert ist, für den Datenabruf verwendet werden kann, führt auch zu einer einheitlichen Gestalt aller Informationen (Sofern man sich um ein vernünftiges Corporate Design gekümmert hat). Der Browser ermöglicht zudem einen 1:1-Ausdruck der WWW-Dokumente.
- Ein recht neuer Begriff ist *Data Warehousing*, worunter man allgemein ein Konzept versteht, das dazu dient, Informationen aus den unterschiedlichsten heterogenen Hardware- und Software-Systemen zu gewinnen. In Mittelpunkt stehen dabei Datenbank- und Informationssysteme. Während man zum Intra-Web-Publishing nur einen Texteditor (für die Erstellung von Webdokumenten) und einen Browser (für die Kontrolle) benötigt, muß für Data Warehousing für jede Datenbank etc. eine passende Konvertierungs-Software erstellt werden.

### 5.3 Interaktion mit dem Benutzer

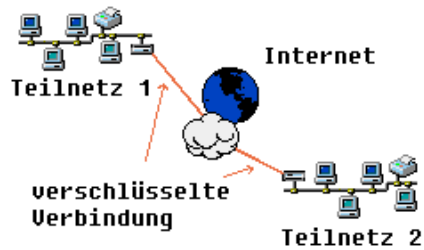
Alles, was früher mit Papier-Formularen erledigt wurde, kann ebenfalls über das Intranet abgewickelt werden, z. B. Urlaubsanträge, Bestellungen, Reiseanträge, Überstundenabrechnungen, Kursanmeldungen, etc. HTML kennt für solche Zwecke sogenannte FORMs (Formulare), bei denen man Eingabefelder, Auswahlmenüs, Kästchen zum Ankreuzen, etc. gestalten kann. Die Formulare werden dann auf dem WWW-Server über spezielle Programme ausgewertet (CGI = Common Gateway Interface). Auch Datenbankabfragen werden so realisiert, wobei hier gleich das Ergebnis zurückgeliefert wird. Um den Benutzern den Umstieg von ihren alten Programmen zum neuen WWW-Interface zu erleichtern, kann man die Web-Formulare gestalterisch an die gewohnte Erscheinungsweise der Eingabe anpassen.

### 5.4 Vom Intranet zum Extranet

Das Intranet läßt sich jederzeit nach außen öffnen, indem man sich Anbindung an einen Provider sucht. Dann kann auf das interne WWW-Angebot auch von außen zugegriffen werden - aber das kostet dann halt auch etwas extra. Im Gegensatz zur vollen Öffnung ins Internet wird das Extranet so

## INTERNET - Möglichkeiten und Dienste

definiert, daß nur bestimmte Systeme (z. B. Kunden oder Vertragshändler) auf die Infos zugreifen dürfen.



Realisiert kann ein solches Extranet durch ein VPN (Virtual Private Network) werden. Ein VPN ist ein gesicherter Kommunikationskanal, der über öffentliche Netze (Internet, aber auch Frame-Relay oder ATM) etabliert wird. Aus dieser sehr allgemeinen Definition lassen sich die beiden Hauptcharakteristika eines VPN ableiten:

- Datenverschlüsselung, da die Daten über ein öffentliches Netz geleitet werden
- Sichere Authentifizierung der Benutzer, die auf Daten im Firmennetz zugreifen wollen

VPNs erlauben es Unternehmen, private WANs aufzubauen, ohne dafür die realen Kosten zahlen und ohne das technische Know-How einkaufen zu müssen. Am Übergang zwischen den lokalen Netzen der einzelnen Niederlassungen zum Internet werden VPN-Server eingerichtet, die ausgehende Daten verschlüsseln und eingehende Daten entschlüsseln. Per VPN lassen sich aber nicht nur zwei oder mehr Standorte mit lokalen Netzen verbinden, sondern auch Kunden oder Zulieferer ins Unternehmensnetz einbinden (Extranet). Eine dritte Möglichkeit bietet sich mit der Einbindung von Aussendienst- und Telearbeitern ins Firmen-LAN (Remote-Access-VPN).

Im ersten Fall hat jeder Standort seinen VPN-Server als Internet-Gateway, meist ein Firewallsystem. Authentifizierung geschieht zwischen den Servern. Bei einem Extranet-VPN finden Verschlüsselung und Authentifizierung zwischen Firewall und dem VPN-Client statt, also auf Benutzerebene. Desgleichen bei Remote Access.

Die neueste Entwicklung stellen Intranet-VPNs dar. Darunter versteht man die Möglichkeit, innerhalb eines Unternehmens wichtige Informationen zu schützen. Dort greifen Benutzer auf Server zu, die ihre Daten verschlüsseln und den Benutzern Zugriff nur auf einzelne, der Sicherheits-Policy entsprechende Server, Dienste und Daten ermöglichen.

---

[◀ Zum Inhaltsverzeichnis](#)

[▶ Zum nächsten Abschnitt](#)

---

Copyright © Prof. Jürgen Plate, Fachhochschule München



## INTERNET - Möglichkeiten und Dienste

*Prof. Jürgen Plate*

---

# 6 Internet-Technik

In diesem Kapitel gehe ich etwas genauer auf die Technik ein, die hinter dem Internet steckt.

Die Verbindung von Rechnern miteinander ist kein Problem mehr. Innerhalb eines Gebäudes nimmt man Kabelverbindungen (Ethernet, Token Ring etc.), für weiter reichende Verbindungen gibt es Modems, Datex-P, ISDN oder Standleitungen. Diese Verbindungen haben aber alle eine unterschiedliche Software-Schnittstelle. Genau um dies zu vermeiden wird im Internet das TCP/IP-Protokoll (Transmission Control Protocol/Internet Protocol) verwendet. Es ist:

- Unabhängig von der darunterliegenden physischen Netzhardware,
- netzweit einheitliche Adressen,
- einheitliche, geschlossene Programmierschnittstelle,
- standardisierte Protokolle für die Netzwerkdienste,
- unabhängig von Herstellern.

## 6.1 Denken in Schichten

Um die Entwicklung und das Verständnis von Rechnernetzen zu erleichtern, hat die ISO ein Modell für Rechnernetze entwickelt, das OSI-Referenzmodell. Dieses Modell teilt den Datenverkehr über ein Rechnernetz in sieben übereinanderliegende Schichten ein, die einander zuarbeiten und jede für sich eine bestimmte Abstraktionsebene kennzeichnen. Wenn Daten zwischen zwei Rechnern übertragen werden, erscheint es im Denkmodell so, als würden zwei gleiche Schichten auf verschiedenen Rechnern miteinander kommunizieren. Die Details der darunterliegenden Ebenen werden vor den darüberliegenden Schichten verborgen.

Beispielsweise ist es die Aufgabe einer Schicht, eine fehlerfreie Verbindung zwischen zwei benachbarten Netzknoten zur Verfügung zu stellen. Das bedeutet, daß die darüberliegende Schicht sich mit den Details der Datenübertragung zwischen zwei Maschinen nicht mehr zu befassen hat. Sie kann mit der gleichen Schicht der Gegenstelle kommunizieren, ohne sich um Einzelheiten der Datenübertragung und möglicherweise auftretende Fehler kümmern zu müssen. In Wirklichkeit besteht jedoch die einzige Verbindung zwischen zwei Rechnern immer nur auf der Ebene 1, der physikalischen Schicht.

Wenn Daten zu senden sind, werden sie von einer Schicht zur jeweils darunterliegenden Schicht weitergereicht. Damit die einzelnen Schichten voneinander unabhängig sind, müssen die Schnittstellen zwischen den Schichten natürlich bekannt und definiert sein (Wartbarkeit, Fehlersuche). Auch TCP/IP hat einen schichtweisen Aufbau, auch wenn es nicht so stark unterteilt ist wie das OSI-Modell; üblicherweise unterscheidet man vier Schichten. Die Grundlage bildet auch hier die Netzwerkschicht, deren Aufgabe der eigentliche Datentransport ist. Im Gegensatz zu anderen ist TCP/IP kein Netzwerkprotokoll, das die Hardware direkt ansteuert, denn die Aufgabe von TCP/IP ist es ja gerade, die Verwendung solcher Netzwerke zu vereinheitlichen. TCP/IP-Daten werden über ein vorhandenes Trägernetz übertragen, etwa Ethernet, X.25 oder per PPP über Modems. Im OSI-Modell deckt die Netzwerkschicht normalerweise die Hardwareschichten 1 und 2 ab.

Mehr über die Protokolle des Internet, ihre Funktionsweise und die technischen Hintergründe sind im [Skript Computernetze](#) zu finden. Wichtig sind hier vor allem die beiden Kapitel:

### **6.2 TCP/IP**

### **6.3 Höhere Protokolle**

## 6.4 Neuere Entwicklungen

Man müßte Wahrsager sein, um in einer turbulenten Zeit, wie sich die vergangenen Jahre präsentierten, Voraussagen mit hoher Trefferquote machen zu können. Dennoch und gerade zum Milleniumswechsel drängen sich Zukunftsfragen in besonderem Maße auf.

### Das neue Internet-Protocol (IPv6)

Nachdem der Ansturm auf das Netz ungebremst weitergeht und, wie Sie inzwischen wissen, jeder Rechner seine individuelle IP-Adresse haben muß, drohen - wie schon erwähnt - langsam die IP-Nummern zur Neige zu gehen. Eigentlich stehen noch genügend Nummernkreise zur Verfügung, jedoch sind diese in festen Händen. Als die Nutzerzahl im Internet noch relativ gering war, ist man oft zu verschwenderisch mit den IP-Adressen umgegangen, beispielsweise um das Routing zu vereinfachen. Inzwischen werden die C-Netze noch in kleinere Unternetze aufgeteilt, um möglichst ökonomisch mit den Adressen umzugehen. Aber man macht sich bereits Gedanken über neue Formen der Kommunikation und über neue Adressierung im Internet. Mit der kommenden Version IPv6 stehen 128 Bit für die IP-Nummern zur Verfügung und das ist mehr als genug. Je mehr Teilnetze eingebunden werden, desto umfangreicher werden auch die Informationen, die von den Knotenstationen, den Routern, verarbeitet werden müssen. Bei jedem Datenpaket muß ein Router entscheiden, wohin das Datenpaket weitergeschickt werden soll. Je größer die Routingtabellen werden, desto schneller muß die Hardware im Router sein. IPv6 wird auch hier für Abhilfe sorgen. Jeder Internet-Provider bekommt eine feste Teiladresse, in etwa vergleichbar mit der Vorwahl eines Landes oder einer Stadt. Damit müssen den Routern nicht mehr alle Teilnetze bekannt sein, sondern nur noch die Präfixe. Mit einem vergleichbaren Verfahren arbeitet man übrigens heute schon, um die Routingtabellen auf ein erträgliches Maß zu begrenzen.

IPv6 schafft die Grundvoraussetzung dafür, daß Mitteilungen, Bilder, Videos oder Zahlungsströme über die Grenzen der unterschiedlichen Betriebssysteme und Hardwaresysteme hinweg transportiert werden können. Doch wesentliche Anforderungen an ein zeitgerechtes Protokoll, können vom derzeitigen IP nicht erfüllt werden:

- ein Adressraum für den gesamten Globus
- nachvollziehbare (feste) Adresse jedes Teilnehmers
- Verschlüsselung der übertragenen Daten
- rechtzeitige Zustellung zeitkritischer Informationen (On-Demand-Dienste, Telefonie, ...)
- Einsetzbarkeit auch in Funknetzen und Satellitennetzen.

Nicht jede dieser Forderungen an eine neues Protokoll bleibt unwidersprochen. Die starke kryptografische Verschlüsselung ist den "Sicherheitsdiensten" ein Dorn im Auge. Die nachvollziehbare (feste) Adresse jedes Teilnehmers am Internet scheint eine notwendige Einrichtung, wenn sich Dienste wie Internettelefonie etablieren wollen, stört aber die Datenschützer.

### Kein Engpaß an Bandbreiten

Für die Beschreibung von Kommunikationsmedien kann man drei zentrale Parameter verwenden: Die Bandbreite, also die Anzahl der pro Sekunde übertragenen Bits, die Entfernung, die mit der Leitung überbrückt werden kann, die Ausbreitungsgeschwindigkeit der Daten in der Leitung. Bei einer Verbindung im Internet durchlaufen die Daten in der Regel mehrere Router und zwischen diesen Routern gibt es Leitungen mit ganz unterschiedlicher Bandbreite und Netzlast (wenn sich mehrere Verbindungen eine Leitung teilen, sinkt natürlich die Übertragungsrate für jede einzelne Verbindung). Den 'Flaschenhals' bildet dabei immer die Verbindung mit niedrigster Bandbreite. Manche kleine Provider sind beispielsweise über ISDN (128000 Bit/s) angebunden. Wenn dort einige Benutzer größere Dateien per FTP holen, ist die Verbindung schnell 'dicht'. Üblich sind heute Verbindungen zwischen Provider und 'Überprovider' mit 1 oder 2 MBit/s, manchmal auch 4 MBit/s. Letztere habe

## INTERNET - Möglichkeiten und Dienste

dann meist eine dicke Leitungen mit 34 MBit/s. Mit Glasfasertechnik sind derzeit Leitungen im GBit-Bereich (1 GBit = 1 Giga-Bit" = 1000 MBit/s) möglich, wobei höhere Raten in den kommenden Jahren sehr wahrscheinlich sind.

Das zukünftige Internet ist multimedial. Videoströme, Animationen, Photos und Audiodokumente gehören zum guten Ton eines Web-zentrierten Informationsangebotes. Daß zur Übertragung von Bewegtbildern entsprechende Bandbreiten benötigt werden, die sich um das Vielfache dessen bewegen, was "nackte Texte" beanspruchen, ist hinlänglich bekannt. Zitat (1998): *"A couple of years ago, 34 Mbit/s would have been the standard for city-to-city links. Now, it is 155 Mbit/s and in a five years it will be 10 Gbit/s."*

Die Telekommunikationsindustrie hat mehr zu bieten, als sie derzeit auf den Markt bringt. Potentiellen Anbieter sind beispielsweise:

- Bahnbetreiber (Lokal- Fern- und Untergrundbahnen),
- Energieversorger (Elektrizität, Öl und Gas),
- Kabelbetreiber,
- klassischen Telekommunikationsunternehmen und
- Wasser- und Abwasserunternehmen

### **Datenkompression: hohe Qualität bei sinkendem Bedarf an Bandbreite**

Die Aussendung von Audio- und/oder Videosignalen (z. B. Radio-/Fernsehprogramme) über Internet bedarf wegen der erforderlichen hohen Bandbreite und geringen Ende-zu-Ende-Verzögerung

- eines effizienten Kompressionsverfahrens.
- eines Protokolls zum Ausgleich von Datenverlusten und schwankenden Übertragungsraten.

"Streaming" bezeichnet das Abspielen von Audio-/Videodaten in Echtzeit. Ein gebräuchliches Format für Audiodateien ist MP3. "RealAudio" und "RealVideo" sind proprietäre und nicht offengelegte Verfahren von Real Networks. Die Empfangssoftware ist frei erhältlich und in die meisten modernen Web-Browser als Plugin integriert. Das Verfahren ist sehr effizient und kann niedrige Videoauflösungen bereits mit ModernVerbindungen von 14 Kbit/s übertragen.

Geradezu kompletär zum Bandbreiten-Bedarf entwickeln sich moderne Methoden der Datenkompression. Am erfolgreichen Beispiel von MP3 (MPEG 2 Layer 3) kann gezeigt werden, daß trotz der Reduktion der Datenmenge auf 10% des unkomprimierten Audio-Originals, akzeptable Qualitäten erreicht werden können. Ähnliche Entwicklungen sind auch im Bereich der Stand- und Bewegtbilder bekannt und abzusehen.

### **Die Medien konvergieren**

Sowohl auf der technischen Ebene, wie auf der Medienebene zeichnet sich ein "Zusammenwachsen" ab. Auch aus anderen digitalen Kommunikationsnetzen können digitale Telekommunikationsendgeräte mit Display auf das Internet zugreifen, wenn diese Netze mit einem Gateway zum Internet versehen sind. Zwischen Endgerät und Gateway wird dabei das Protokoll WAP (Wireless Application Protocol) benutzt, das Gateway setzt dieses z. B. nach HTTP um. Spezielle Web-Seiten, die mit Tags der Beschreibungssprache WML (WAP Markup Language) versehen sind, können vom Gateway wiederum in WAP-Nachrichten umgesetzt werden und sind damit vom Telekommunikationsendgerät abrufbar. WAP und WML sind Beispiele für den mobilen Zugang zum Internet. Ericsson und Microsoft, Nokia und Macromedia haben ihre Zusammenarbeit für ein mobiles Internet erklärt. Telefonieren, sich Informieren, Lesen und Unterhaltung werden zu einem Medienkonglomerat verschmelzen.

## INTERNET - Möglichkeiten und Dienste

Das Real-Time Transport Protocol RTP ist ein Protokoll der Transportschicht zur Übertragung zeitkritischer Daten, es setzt auf IP auf. RTP kann zusammen mit beliebigen Kompressionsverfahren zur Realisierung von Audio-/Videodatenströmen genutzt werden. RTP ist auch Bestandteil des Java Media Framework.

### Kryptographie

Nach anfänglichen Hindernissen der Nutzung kryptographischer Techniken, einerseits bedingt durch Exportrestriktionen der US-Regierung, andererseits durch das Verbot der Anwendung in einigen Ländern (z. B. Frankreich) scheint sich eine umfangreiche Nutzung zu etablieren.

Kryptographische Methoden bilden die Basis für die Sicherheit der Übertragung von Daten aller Art (Texte, Bilder, Tondokumente, usw.) gegen:

- das "Abhören" (Empfangen durch Unberechtigte),
- die Verfälschung und
- das Vorspiegeln unwahrer Absender (= digitale Signatur)

Damit wird der Grundstein für den elektronischen Zahlungsverkehr, die Kontraktfähigkeit digitaler Dokumente, die untrennbare Kennzeichnung der Daten mit Urheberinformationen oder Lizenzinhabern (Watermarking) gelegt.

### Applikationen

Peer-to-Peer-Computing (P2P) übers Netz ist nicht mehr zu stoppen und gilt selbst bei VCs als absolut "hot" Napster, Gnutella und Co. bringen die Nutzer fürs Filesharing direkt in Kontakt miteinander. Was heute fürs MP3-Tauschen gut ist, könnte in Zukunft auch das Modell sein für den mittelsmannlosen E-Commerce, das unkomplizierte Publishing oder die Echtzeit-Suche nach Informationen in den wachsenden Datenbergen.

Napster, das inzwischen von rund 20 Millionen Netzbewohnern genutzt wird, macht Lust auf mehr. Applikationen wie Gnutella und FreeNet ermöglichen seit dem Frühjahr 2000 das Filesharing beliebiger Dateien - also auch von kompletten Videos oder digitalen Büchern. Selbst einen zentralen Verbindungsserver - die Bedingung für jegliche Webkommunikation - braucht es nicht mehr, da durch beide Programme die vernetzten Rechner der User selbst zu "Servern" umgewandelt werden und in Echtzeit dort nach Material von Interesse gesucht werden kann.

Doch die punktgenaue Peer-to-Peer-Revolution, die letztlich an die Zeiten des Internet vor dem Web anknüpft, als die Netzpioniere in den Universitäten oder großen Firmen noch ihre eigenen Rechner als Downloadstationen und Knoten im Cyberspace positionierten, geht weit über den in Mode gekommenen MP3-Austausch hinaus. Letztlich könnte ein Großteil der Aktivitäten, die heute noch über das Web abgewickelt werden, wieder gänzlich von den Nutzern selbst in die Hand genommen werden.

Andere denken an das, was ich als 'Internet für Waschmaschinen' bezeichne. Jedes Gerät im Haus soll über einen Netzwerkananschluß verfügen und in der Industrie wird bereits über das 'smart house' diskutiert.

### Links

<http://www.napster.com/>  
<http://freenet.sourceforge.net>  
<http://www.applesoup.com/>  
<http://www.mpaa.org/>

<http://gnutella.wego.com/>  
<http://gnutella.nerdherd.net>



[Zum Inhaltsverzeichnis](#)



[Zum nächsten Abschnitt](#)

---

Copyright © Prof. Jürgen Plate, Fachhochschule München



## INTERNET - Möglichkeiten und Dienste

*Prof. Jürgen Plate*

---

# 7 Suchen im Internet

*"Everything you need to know is on the Internet. You just can't find it."*

*Anonymous*

Ein großer Vorteil des Internet ist, daß man dort Dokumente schnell und einfach publizieren kann. Für den Publikationsprozeß und die publizierten Inhalte ist allein der Autor verantwortlich. Die Qualität der angebotenen Inhalte ist daher sehr unterschiedlich. Das WWW als Teil des Internet bietet eine große Menge an wissenschaftlichen Informationen. Forschungsberichte, Seminarunterlagen, Dissertationen, akademische Schriften jeglicher Fachdisziplin sind schnell und mit einem sehr hohen Aktualitätsgrad verfügbar. Auch zahlreiche Broschüren, Arbeitsberichte, Protokolle von Vereinen, Verbänden und Parteien sind über das Internet schnell und aktuell zu bekommen. Die wichtigsten Probleme bei der Informationssuche sind:

- die fehlende Organisation: es gibt keine zentrale Koordination oder Kontrolle, wer, wo, was und wie veröffentlicht. Das ist aus Sicht des Suchenden zwar bedauerlich, ist aber andererseits ein wesentlicher Garant für die Vielfalt der Angebote und den leichten Zugang für alle potentiellen Anbieter.
- die fehlende Strukturierung: eine 'Veröffentlichung' im Internet kann ein kurzer Text, eine Grafik, ein ganzes Buch oder eine gigabytegroße Datenbank sein - aber all diese verschiedenen Veröffentlichungsweisen stehen gleichberechtigt nebeneinander, ohne daß eine Vorauswahl möglich ist. Informationen über solche Veröffentlichungen stehen meist nicht für eine gezielte Suche zur Verfügung (z. B. Inhaltsangaben, Informationen über Autor, Erstellungsdatum, Quellen etc.).
- die Beliebigkeit: ob eine Information im Internet zu finden ist, ist oftmals Zufall und hängt davon ab, ob jemand Zeit, vielleicht auch Geld, in jedem Fall aber ein Interesse daran hat, sie zu verbreiten.
- die Dynamik: täglich kommen neue Angebote im Internet hinzu, und das, was einmal existiert hat, kann wieder verschwinden, verändert, gelöscht oder verschoben werden.

## 7.2 Wie funktionieren Suchmaschinen?

Zunächst jedoch erfahren Sie wie die Suchmaschinen an ihre Informationen kommen. Die Kenntnis der verschiedenen Strukturen von Suchmaschinen ist die erste Voraussetzung für eine erfolgreiche Recherche. Die wichtigsten Suchsysteme des Internet arbeiten mit zwei Verfahren:

1. gibt es die automatische Volltextindexierung von Internet-Dokumenten (das machen zum Beispiel Alta Vista, HotBot, oder Infoseek)
2. gibt es Dienste, die die Internet-Ressourcen systematisch, klassifikatorisch, oder hierarchisch aufgliedern (wie zum Beispiel Yahoo, DINO oder Web.de)
3. Daneben existieren noch weitere Ansätze. So beschränken sich manche Dienste auf das Verzeichnen von Teilbereichen (wie zum Beispiel der *Commercial Sites Index* auf Unternehmen im Internet). Andere Suchdienste setzen nicht auf eine möglichst große Zahl indexierter Dokumente, sondern auf eine differenzierte Bewertung dieser Dokumente (beispielsweise Magellan).

Bei der Volltext-Indexierung wird der gesamte Text der Web-Seiten indexiert. Die Indexierung verläuft automatisch. Für den Input sorgen sogenannte *Robots* oder *Spider*. Dies sind Programme, die selbständig arbeitend Ressourcen im Internet "aufspüren", indem sie Verweisen (Hyperlinks) von bereits bekannten Dokumenten folgen. Jedes neu von einem solchen Robot gefundene Dokument wird automatisch in der Datenbank der Suchmaschine verschlagwortet. Wie dies geschieht, hängt vom einzelnen Robot ab; manche indexieren den HTML-Titel oder die ersten Absätze eines Dokuments;

## INTERNET - Möglichkeiten und Dienste

andere durchforsten das gesamte Dokument und indexieren buchstäblich jedes Wort. Die meisten Suchmaschinen speichern die gesammelten Dokumente nicht als komplette Spiegelung. Dazu bedarf es eines gigantischen Rechen- und Speicheraufwandes, den derzeit nur Alta Vista betreibt. Zur Suche wird eine Indextabelle angelegt, die die Worte einer Seite in einer Ja-Nein-Struktur enthält. Hierdurch kommen verschiedene Eigenschaften der Suchmaschine zustande:

- Hohe Suchgeschwindigkeit, da in der Tabelle nur per Ja-Nein-Suche auf das Vorhandensein des gesuchten Wortes abgefragt wird. Ja führt zu Treffern, Nein entsprechend nicht.
- Wortbedeutungen spielen keine Rolle. Bei der Suche nach "Macht" wird auch das Dokument "Geld allein macht glücklich" gelistet, obwohl es inhaltlich nichts mit dem Suchwort zu tun hat. Abhilfe würde in diesem Fall die Eingabe des großgeschriebenen Suchwortes schaffen, sofern die Suchmaschine Groß- und Kleinschreibung unterscheidet.
- Worte, die im Plural anders geschrieben werden, werden nicht gelistet. "Schrank" und "Schränke" sind wegen des Umlautes zwei verschiedene Worte.
- "Kuchen" und "Gebäck" sind zwar inhaltlich eng verwandt, aber verschiedene Worte. Die Suche nach dem einen wird keine Treffer beim anderen hervorrufen. Diese Verbindung schaffen nur redaktionell bearbeitete Suchkataloge wie z.B. Yahoo.

Ein für die Abfrage bedeutsamer Unterschied liegt darin, ob die Suchmaschinen alle Begriffe, auch sogenannte Stopwörter wie "der", "die", "das", "und", "ob", "ein", "ich" indexieren, oder ob sie sich auf sogenannte Schlüsselwörter beschränken, die wichtige Informationen eines Dokumentes tragen. Beides hat Vor- und Nachteile: Mit Suchmaschinen, die alle Begriffe indexieren, können Sie auch nach Phrasen wie "to be or not to be" suchen, eine Phrase, die - wengleich klassisch - nur aus Stopwörtern besteht. Andererseits verlängert die Indexierung aller Wörter die Dauer einer Suchanfrage natürlich beträchtlich, weil die Datenmenge, die bei einer Anfrage durchforstet werden muß, um ein Vielfaches größer ist. Die einzelnen Suchdienste unterscheiden sich außerdem darin, wie weitgehend ihre Robots und Spider Dokumente indexieren; sie unterscheiden sich in der Indexierungsbreite (wie viele unterschiedliche Dienste/Server werden durchforstet) und in der Indexierungstiefe (wie tief dringt ein Robot in die Angebots- und Verzeichnisstruktur eines Webangebotes ein).

Sucht man in einem auf Volltext-Indexierung basierenden Suchdienst nach einem beliebigen Begriff, verweist die Suchmaschine auf alle Dokumente, die sie durchsucht hat und die den gesuchten Begriff enthalten. Die Suchdienste geben als Ergebnis gleich die URLs der gefundenen Dokumente als Hyperlinks aus, so daß Sie sofort das gefundene Dokument aufsuchen können. In vielen Fällen bekommen Sie jedoch nicht nur einen Treffer, je nach Suchbegriff meldet Ihnen die Suchmaschine mehrere Tausend von Treffern. Um die Auswahl aus mehreren Treffern zu erleichtern, nehmen die meisten, auf Volltext basierenden Suchmaschinen eine automatische Gewichtung der Suchergebnisse vor, das sogenannte "Ranking". Die Suchmaschine gewichtet die Ergebnisse auf der Basis eines mathematischen Verfahrens, der unter anderem die Häufigkeit des gesuchten Begriffs im Dokument bewertet. Es gibt keine generelle Gewichtung; jede Suchmaschine verwendet zur Feststellung der Relevanz eines Suchtreffers unterschiedliche Mechanismen. Im Suchergebnis erscheint die Liste der Treffer bei manchen Suchdiensten nach Prozenten gewichtet. Bei anderen Suchdiensten stehen einfach ohne weitere Angaben die "besten" Treffer am Anfang. Die verschiedenen Hauptaspekte sind:

1. Anzahl der übereinstimmenden Wörter Werden mehrere Suchworte verknüpft, so werden Ergebnisse, die alle oder viele der gesuchten Begriffe oder Phrasen enthalten, als relevanter eingestuft.
2. Häufigkeit des Vorkommens von Suchbegriffen Je öfter das Suchwort im Dokument vorkommt, desto wichtiger wird es für den Gesamthalt des Dokumentes gewertet.
3. .Domain und URL: Auf Systemen, die lange Dateinamen zulassen, werden Dokumente oft unter einem aussagekräftigen Namen gespeichert. Die Indexierungssoftware wertet das Dokument bei Übereinstimmung mit dem Suchwort als besonders relevant. Das gilt ganz besonders, wenn es sich um den Domainnamen handelt.
4. Titel: Ein Dokument, mit dem Suchwort im Titel hat gute Chancen auf einen vorderen Platz.

5. Überschrift: Enthält eine Überschrift das gesuchte Wort, befaßt sich das gesamte Dokument oder ein wesentlicher Teil damit.
6. Meta-Tag: Die Maschinen, die den Meta-Tag auswerten, ordnen Dokumente, die den Begriff im Content- (Inhalt) oder Keywords (Schlüsselworte)-Tag führen, höher ein.
7. Dokumentenanfang: Je früher das Wort im Dokument auftaucht, desto relevanter für das Suchergebnis wird es gewichtet.
8. Bezahlung: Manche wenige Suchmaschinen setzen gegen Bezahlung bestimmte Links nach vorne.

Das Ranking grenzt zwar die Suchergebnisse ein, liefert aber dennoch in vielen Fällen eine unübersichtliche Anzahl von Treffern mit über 90-prozentiger Genauigkeit. Dabei ist allerdings keineswegs garantiert, daß die einzelnen Ergebnisse wirklich alle mit dem zu tun haben, was Sie suchen. Selbst bei einer Treffergenauigkeit von 99 Prozent kann es sein, daß es in der Fundstelle nicht wirklich um die Frage geht, auf die Sie eine Antwort suchen.

### 7.2 Erster Grundsatz beim Suchen

Die Recherche nur beginnen, wenn das Internet als richtiges Medium für die Suche in Frage kommt. Überlegtes Handeln und ein bißchen Organisation sind bei der Recherche im Internet die ersten Schritte zum Erfolg. Denn es gibt weder die eine Suchmaschine, die das ganze Internet erfaßt, noch die eine geniale Suchmethode, die immer funktioniert. Doch die erste Vorüberlegung, bevor man sich überhaupt an den Computer setzt, lautet: Ist das Internet überhaupt das am besten geeignete Medium zur Suche nach den gewünschten Auskünften? Als nächstes muß man sich Gedanken darum machen, was genau gesucht wird. Von der Antwort dieser durchaus nicht trivialen Frage hängt das weitere Vorgehen ab, und damit sind das Wo und das Wie der Suche vorgegeben. Leitkategorien lassen sich für eine grobe Gliederung heranziehen. Klar definieren, was gesucht wird:

- Eine Firma, eine Organisation, eine Person, ein Produkt, einen Gegenstand, ein abstraktes Konzept oder ein
- theoretischer Begriff.
- Festlegen der Suchmaschine(n) bzw. Suchprogramm(e).
- Formulieren der einzelnen Suchbegriffe.
- Kontrolle der erhaltenen Informationen.
- Falls nötig, verbessern der Suchparameter nach dem ersten Durchlauf.

### 7.3 Wann lohnt sich die Suche im Internet?

Eine Suche im Internet ist nicht immer von Erfolg gekrönt. Das allein wäre nicht so schlimm, aber zum Zeitpunkt dieser Erkenntnis ist oft bereits eine Menge wertvoller Zeit und Geld für Online- und Telekom-Gebühren vertan. Um solchen Ärgernissen zu entgehen, sollten Sie von vornherein überlegen, ob das Internet das richtige Medium für Ihre Recherche ist. Diese Rat mag zwar überflüssig erscheinen, doch es kommt immer wieder vor, daß man genau aus diesem Grund wertvolle Zeit vor dem Rechner vergeudet.

Während genau definierbare, thematisch gut abzugrenzende Begriffe relativ leicht zu finden sind, macht insbesondere die Suche nach komplexen Konzepten mit vielen thematischen Verknüpfungen sehr viel Mühe. Ein weitverzweigter Themenkomplex muß erst in einzelne Teilgebiete aufgebrochen werden, und dann muß jedes dieser Teilgebiete individuell nach passenden Dokumenten durchforstet werden. Um es kurz zu machen: Dieser Zeitaufwand lohnt sich im Normalfall nicht. Ziehen Sie in solchen Fällen lieber Kollegen, Experten oder Fachliteratur zu Rate. Tip für diesen Fall: Versuchen Sie Ihr Glück mit einer schnellen Anfrage, denn es gibt durchaus die Chance eines Zufallstreffers, aber lassen Sie sich nicht in eine lange, erfolglose Suche nach weitverzweigten Inhalten ein.

## 7.4 Suchmaschinen versus Verzeichnisse

Ein möglichst umfassender Nachweis von Web-Dokumenten ist über Suchmaschinen möglich, die in Einzelfällen bis zu 60 Mio. Web-Seiten nachweisen. Einfache Suchfragen, die aus ein oder zwei Suchbegriffen bestehen, führen hier aber i.d.R. bereits zu unübersichtlichen Treffermengen. Als grobe Regel gilt, daß Suchmaschinen erst bei Suchfragen mit drei oder mehr Suchbegriffen einigermaßen problemlos anwendbar sind. Sie sind deshalb vor allem für die Beantwortung spezieller Fragestellungen gut geeignet.

Wie verfährt man aber bei allgemeineren Fragestellungen? Bei einer gründlichen, umfassenden und aktuellen Suche wird man auch hier auf Suchmaschinen nicht verzichten können. Fast alle bieten sinnvolle Möglichkeiten der Einschränkung von Suchfragen. In vielen Fällen auch ausreichend ist die Heranziehung von Auswahlsammlungen oder 'Verzeichnissen', die intellektuell erstellt bzw. bearbeitet werden. Auch diese haben Nachteile: Ihre Aktualität läßt fast immer zu wünschen übrig. Obwohl die meisten von ihnen eine Abfrage nach Suchbegriffen zulassen, sind sie nur beschränkt über sog. "Meta-Suchmaschinen" gemeinsam recherchierbar. Schließlich ist auch die beste Auswahl dem Verwurf der Subjektivität ausgesetzt.

## 7.5 Suchmaschinen richtig bedienen

Suchmaschinen arbeiten aus Platzgründen mit Indizes, zerlegen also die Texte und Meta-Tags (vom Autor mitgelieferte Suchworte im Vorspann des Webangebotes) der in die Datenbank aufgenommenen Seiten in wenige, mehr oder minder relevante Stichworte. Wenn Sie zumindest eine teilweise Deckung mit einem dieser indizierten Stichworte bei der Suchanfrage erhalten, dann haben Sie einen Treffer gelandet. Je mehr Stichworte aus dem Index mit ihren Suchbegriffen übereinstimmen, um so wahrscheinlicher haben Sie eine inhaltlich passende Seite gefunden.

Um eine möglichst genaue Abfrage zu ermöglichen, erlauben viele Suchmaschinen sogenannte logische Operatoren, wie zum Beispiel UND, ODER bzw. NICHT. In den allermeisten Fällen werden nicht anders gekennzeichnete Wortfolgen als ODER-Verknüpfungen behandelt. Neben diesen Grundoperatoren bieten einzelne Suchmaschinen weitere Hilfsmittel, wie zum Beispiel das einem Wort vorangestellte '+' bei Fireball oder AltaVista, welches die Suchmaschine zwingt, nur Treffer zurückzuliefern, die diesen Begriff genau in dieser Form enthalten. Überlegen Sie sich Stichworte, die möglichst genau den Kern oder das Konzept des von Ihnen gesuchten Begriffes benennen. Falls Sie ausschließlich ODER-Verknüpfungen verwenden, sollten Sie die Suchbegriffe sehr penibel formulieren, zum Beispiel die genaue Typenbezeichnung eines Gerätes eintragen. ODER-Verknüpfungen sind vorteilhaft, wenn Sie nicht exakt wissen, wie die Antwort beschaffen sein soll. Dies trifft beispielsweise bei der Suche nach einem technologischen Konzept zu, dessen Elemente Sie zwar vage umschreiben können, dessen zentrale Fachbegriffe aber unbekannt sind.

## 7.6 So gehen Sie bei der Suche vor

- Überprüfen Sie Ihre Schreibweise!  
Falls Sie auf Ihre Anfrage kein Ergebnis bekommen, schauen Sie, ob Sie Ihre Suchbegriffe richtig geschrieben haben. Überprüfen Sie auch, ob Sie sich an die Groß- und Kleinschreibung gehalten haben. Manche Suchdienste unterstützen die Unterscheidung zwischen Groß- und Kleinschreibung. Dann steht zwar jeder Kleinbuchstabe auch für einen Großbuchstaben aber nicht umgekehrt.
- Verzichten Sie auf häufig gebrauchte Wörter!  
Zu Wörtern wie "Programm" oder "Microsoft" findet eine große Suchmaschine mehr als 10.000 Fundstellen, die Ihnen keine Informationen bieten. Versuchen Sie also, auf solche häufig gebrauchten Wörter zu verzichten. Weniger ist hier mehr!
- Nutzen Sie die Phrasensuche!  
Wenn Sie beispielsweise nach einer Person suchen, suchen Sie sie als Phrase.

## INTERNET - Möglichkeiten und Dienste

- Grenzen Sie Ihre Suche ein!  
Über die logischen Verknüpfungen stehen Ihnen eine ganze Reihe von Möglichkeiten zur Verfügung, um Ihre Suche einzugrenzen und zu präzisieren.
- Schließen Sie aus, was Sie nicht erfahren wollen!  
Es gibt Begriffe, die in Zusammenhang mit einem weiteren Begriff als Begriffspaar sehr häufig vorkommen. Schließen Sie den Teil einer Wortkette aus, der mit Ihrer Frage nichts zu tun hat; Sie ersparen sich so viele unnütze Treffer. Bei vielen Suchsystemen kann man auch ganze Domains von der Suche ausschließen.
- Nehmen Sie möglichst viele Begriffe für Ihre Suchanfrage, aber nicht zu viele!  
Je mehr Begriffe Ihre Suchanfrage enthält, desto präziser können Sie suchen. Aber Vorsicht: Grenzen Sie Ihre Suche nicht mit zu vielen Suchwörtern so ein, daß Sie das gewünschte Dokument vielleicht gar nicht finden können. Die Eingrenzung kann gleichzeitig eine Ausgrenzung sein. In einzelnen Fällen gilt es abzuwägen, welche Begriffe nötig sind, um die Suche einzuschränken, und welche Begriffe nicht gefragt werden sollten, um das Ergebnis nicht zu sehr zu beschränken. Probieren Sie es einfach aus, mit der Zeit bekommen Sie mehr und mehr ein Gefühl dafür, wie Sie eine sinnvolle Anfrage aufbauen können.
- Finden Sie deutschsprachige Dokumente in internationalen Suchdiensten!  
Wenn Sie einen internationalen Suchdienst nutzen, aber dennoch auch oder nur deutsche Dokumente in Ihrer Ergebnisliste sehen möchten, ergänzen Sie Ihre Anfrage durch einen deutschsprachigen Begriff.
- Übersetzen Sie Ihre Anfrage ins Englische für die internationalen Suchdienste!  
Aber auch der umgekehrte Fall macht Sinn: Falls Sie mit Ihrer deutschsprachigen Anfrage in einem internationalen Suchdienst nicht erfolgreich sind oder Sie noch mehr Ergebnisse erzielen wollen, übersetzen Sie Ihre Suchanfrage ins Englische. Oft unterscheidet sich auch die Schreibweise von Personennamen oder Orten je nachdem, welche Sprache benutzt wird. Sie bekommen deutlich mehr Ergebnisse, wenn Sie nach beiden Schreibweisen suchen.
- Arbeiten Sie mit Synonymen!  
Falls Sie auf Ihre Anfrage keine Ergebnisse oder nur mangelhafte Treffer erzielen, probieren Sie es mit der Abfrage nach einem sinnverwandten Wort. Die Volltext-Suchdienste verschlagworten nur die Begriffe, die im Dokument stehen.
- Lernen Sie aus Ihren Resultaten!  
Sehen Sie sich Ihre Treffer genau an. Wählen Sie aus, welche Ergebnisse Ihrem Wunsch am nächsten kommen. In den Titeln oder Kurzbeschreibungen dieser für Sie besonders treffenden Ergebnisse kommen vielleicht Begriffe vor, die Sie für eine neue Suche verwenden können oder die Sie auf eine Idee für neue Begriffe bringen. Versuchen Sie mit diesen neuen Begriffen, Ihre Suche weiter einzuschränken und zu präzisieren.
- Lernen Sie die Suchfunktionen mehrerer Suchdienste kennen!  
Die Suchmaschinen unterscheiden sich unter anderem stark darin, mit welchen Suchfunktionen sie aufwarten können. Die Kenntnis mehrerer Suchmaschinen und ihrer individuellen Möglichkeiten erleichtert Ihnen daher eine erfolgreiche Recherche. Kennen Sie mehrere Maschinen, können Sie je nach Bedarf die benötigte Suchfunktion nutzen.
- Freunden Sie sich mit zwei bis vier Suchdiensten an!  
Für den Suchalltag sollten Sie sich zwei bis vier Suchdienste heraussuchen, die Sie für besonders geeignet halten, und diese besonders gut kennenlernen. Beschäftigen Sie sich ausführlicher mit der Syntax oder der Systematik des jeweiligen Dienstes, arbeiten sich ein wenig ein.
- Experimentieren Sie!  
Wenn Sie nicht immer fündig werden, geben Sie nicht auf, sondern probieren Sie etwas Neues. Experimentieren Sie. Stellen Sie eine andere Anfrage, wechseln Sie den Suchdienst, probieren Sie ein Internet-Verzeichnis, wenn Sie sich bislang auf die Volltextsuche beschränkt haben oder umgekehrt. Auch eine gut geplante Suchanfrage kann in einer Sackgasse enden.
- Bewerten Sie die Ergebnisse  
Suchsystem spucken auf Ihre Anfrage hin eine Liste von Links aus. Bei Suchmaschinen sehen Sie noch ca. vier Zeilen aus der jeweiligen Webseite und den zugehörigen Link. Auch wenn

## INTERNET - Möglichkeiten und Dienste

der Text nur kurz und oft nichtssagend ist, bekommt man mit der Zeit ein Gefühl dafür, ob sich eine Weiterverfolgung lohnt. Auch die Herkunft des Links ist wichtig bei der Suche nach wissenschaftlichen Berichten ist eine Hochschuladresse wertvoller, bei der Suche nach einem Produkt eine Firmenadresse.

- Übernehmen Sie wichtige Links in die Bookmarks. Manchmal ergeben sich bei der Suche auch Zufallsfunde zu einem anderen Gebiet, die Sie sich so notieren können.

**Eine ausführliche Anleitung zur Internet-Recherche mit Hintergründen, Tips und vielen Links finden Sie unter <http://www.netzmafia.de/skripten/suchen/>.**



[Zum Inhaltsverzeichnis](#)



[Zum nächsten Abschnitt](#)

---

Copyright © Prof. Jürgen Plate, Fachhochschule München



## INTERNET - Möglichkeiten und Dienste

*Prof. Jürgen Plate*

---

# 8 Anhang

## 8.1 Literaturempfehlungen

### Online-Informationen

Grundinformationen liegen als Verweis auf jedem besseren WWW-Server! Die meisten Autoren verlangen bei Quellenangabe und nicht-kommerzieller Nutzung keine Gebühren.

- Geschichte des Internet
- Elektronische Ausgabe von In acht Sekunden um die Welt
- Suchfibel
- Stefan Muenz: HTML-Dateien selbst erstellen

*Links zur Geschichte:*

<http://www.heise.de/ix/artikel/1995/10/040/>

[http://www.uni-koeln.de/rrzk/kompass/64/wmwork/www/k64\\_15.html](http://www.uni-koeln.de/rrzk/kompass/64/wmwork/www/k64_15.html)

<http://ig.cs.tu-berlin.de/s94/511/Reader/www/B/>

<http://www.xic.de/xlink/geschichte/index.html>

<http://www.xic.de/xlink/menschen/index.html>

<http://www.xic.de/xlink/netz/>

<http://www.xic.de/xlink/produkte/vertraege/index.html>

<http://www.xic.de/xlink/geschichte/frueher/zorn-ueber-xlink.html>

<http://www-zorn.ira.uka.de/zorn/Buchbeitrag251197/Buchbeitrag3000B.html>

<http://www-zorn.ira.uka.de/fridrich/PANiON/iX.html>

<http://www.sub.net/geschichte/>

<http://www.heise.de/tp/deutsch/inhalt/te/1251/2.html>

<http://in.openoffice.de/old/deutsch/verein/ziele.shtml>

### Bücher

Erich Stein:

**Taschenbuch Rechnernetze und Internet**

Fachbuchverlag Leipzig

James F. Kurose/Keith W. Ross:

**Computernetze**

Prentice Hall (Pearson Studium)

Douglas E. Comer:

**Computernetzwerke und Internets**

Prentice Hall (Pearson Studium)

Wolfgang Sander-Beuermann:

**Internet kurz und fündig**

Verlag Addison Wesley

Scheller/Boden/Geenen/Kampermann:

**Internet: Werkzeuge und Dienste**

Springer-Verlag

Paul Gilster:

**Der Internet-Navigator**

Hanser-Verlag

Levine/Baroudi:  
**Internet für Anfänger**  
iwt - Thomson

Peter Klau:  
**Das Internet**  
iwt - Thomson

Harald Lux:  
**Der Internet-Markt in Deutschland**  
dpunkt-Verlag

Vince Emery:  
**Internet im Unternehmen**  
dpunkt-Verlag

Michael Döge:  
**Intranet**  
O'Reilly

G. Eckel/W. Steen:  
**Intranets**  
Hanser-Verlag

Potempa, Franke, Osowski, Schmidt:  
**Informationen finden im Internet**  
Hanser-Verlag

D. J. Barrett:  
**Ganer und Ganoven im Internet**  
O'Reilly

Kai Fuhrberg:  
**Internet-Sicherheit**  
Hanser-Verlag

A. Beutelspacher, J. Schwenk, K.-D. Wolfenstetter:  
**Moderne Verfahren d. Kryptographie**  
Vieweg-Verlag

W. Fumy, H. P. Rieß:  
**Kryptographie**  
Oldenbourg-Verlag

## 8.2 Domain name registries around the world

The list below contains the two-letter TLDs according to IANAs list, all in alphabetical order.

**gTLDs 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**

NOTE: NORID is only administrating the **.no** TLD

## INTERNET - Möglichkeiten und Dienste

<b>gTLDs</b>		
<b>.com</b> <u>Commercial</u>	<b>.ac</b> <u>Ascension Island</u>	<b>.ba</b> <u>Bosnia and Herzegowina</u>
<b>.edu</b> <u>Educational</u>	<b>.ad</b> <u>Andorra</u>	<b>.cc</b> <u>Cocos (Keeling) Islands</u>
<b>.gov</b> <u>US Government</u>	<b>.ae</b> <u>United Arab Emirates</u>	<b>.cd</b> <u>Zaire</u>
<b>.int</b> <u>International Organizations</u>	<b>.af</b> <u>Afghanistan</u>	<b>.cf</b> <u>Central African Republic</u>
<b>.mil</b> <u>US Dept of Defense</u>	<b>.ag</b> <u>Antigua and Barbuda</u>	<b>.cg</b> <u>Congo</u>
<b>.net</b> <u>Networks</u>	<b>.ai</b> <u>Anguilla</u>	<b>.ch</b> <u>Switzerland</u>
<b>.org</b> <u>Organizations</u>	<b>.al</b> <u>Albania</u>	<b>.ci</b> <u>Côte d'Ivoire</u>
	<b>.am</b> <u>Armenia</u>	<b>.ck</b> <u>Cook Islands</u>
	<b>.an</b> <u>Netherlands Antilles</u>	<b>.cl</b> <u>Chile</u>
	<b>.ao</b> <u>Angola</u>	<b>.cm</b> <u>Cameroon</u>
	<b>.aq</b> <u>Antarctica</u>	<b>.cn</b> <u>China</u>
	<b>.ar</b> <u>Argentina</u>	<b>.co</b> <u>Colombia</u>
	<b>.as</b> <u>American Samoa</u>	<b>.cr</b> <u>Costa Rica</u>
	<b>.at</b> <u>Austria</u>	<b>.cs</b> <u>Czechoslovakia mer - non-existing</u>
	<b>.au</b> <u>Australia</u>	<b>.cu</b> <u>Cuba</u>
	<b>.aw</b> <u>Aruba</u>	<b>.cv</b> <u>Cape Verde</u>
	<b>.az</b> <u>Azerbaijan</u>	<b>.cx</b> <u>Christmas Island</u>
		<b>.cy</b> <u>Cyprus</u>
		<b>.cz</b> <u>Czech Republic</u>

---

<b>.de</b> <u>Germany</u>	<b>.ec</b> <u>Ecuador</u>	<b>.fi</b> <u>Finland</u>	<b>.ga</b> <u>Gabon</u>
<b>.dj</b> <u>Djibouti</u>	<b>.ee</b> <u>Estonia</u>	<b>.fj</b> <u>Fiji</u>	<b>.gb</b> <u>United Kingdom</u>
<b>.dk</b> <u>Denmark</u>	<b>.eg</b> <u>Egypt</u>	<b>.fk</b> <u>Falkland Islands</u>	<b>.gd</b> <u>Grenada</u>
<b>.dm</b> <u>Dominica</u>	<b>.eh</b> <u>Western Sahara</u>	<b>.fm</b> <u>Micronesia</u>	<b>.ge</b> <u>Georgia</u>
<b>.do</b> <u>Dominican Republic</u>	<b>.er</b> <u>Eritrea</u>	<b>.fo</b> <u>Faroe Islands</u>	<b>.gf</b> <u>French Guiana</u>
<b>.dz</b> <u>Algeria</u>	<b>.es</b> <u>Spain</u>	<b>.fr</b> <u>France</u>	<b>.gg</b> <u>Guernsey</u>
	<b>.et</b> <u>Ethiopia</u>		<b>.gh</b> <u>Ghana</u>
			<b>.gi</b> <u>Gibraltar</u>
			<b>.gl</b> <u>Greenland</u>
			<b>.gm</b> <u>Gambia</u>
			<b>.gn</b> <u>Guinea</u>
			<b>.gp</b> <u>Guadeloupe</u>
			<b>.gq</b> <u>Equatorial Guinea</u>
			<b>.gr</b> <u>Greece</u>
			<b>.gs</b> <u>South Georgia and the South Sandwich Islands</u>
			<b>.gt</b> <u>Guatemala</u>
			<b>.gu</b> <u>Guam</u>
			<b>.gw</b> <u>Guinea-Bissau</u>
			<b>.gy</b> <u>Guyana</u>

---

## INTERNET - Möglichkeiten und Dienste

<b>.hk</b> <u>Hong Kong</u>	<b>.id</b> <u>Indonesia</u>	<b>.je</b> <u>Jersey</u>	<b>.ke</b> <u>Kenya</u>
<b>.hm</b> <u>Heard and McDonald Islands</u>	<b>.ie</b> <u>Ireland</u>	<b>.jm</b> <u>Jamaica</u>	<b>.kg</b> <u>Kyrgystan</u>
<b>.hn</b> <u>Honduras</u>	<b>.il</b> <u>Israel</u>	<b>.jo</b> <u>Jordan</u>	<b>.kh</b> <u>Cambodia</u>
<b>.hr</b> <u>Croatia</u>	<b>.im</b> <u>Isle of Man</u>	<b>.jp</b> <u>Japan</u>	<b>.ki</b> <u>Kiribati</u>
<b>.ht</b> <u>Haiti</u>	<b>.in</b> <u>India</u>		<b>.km</b> <u>Comoros</u>
<b>.hu</b> <u>Hungary</u>	<b>.io</b> <u>British Indian Ocean Territory</u>		<b>.kn</b> <u>Saint Kitts and Nevis</u>
	<b>.iq</b> <u>Iraq</u>		<b>.kp</b> <u>Korea, Democratic People'spublic of</u>
	<b>.ir</b> <u>Iran</u>		<b>.kr</b> <u>Korea, Republic of</u>
	<b>.is</b> <u>Iceland</u>		<b>.kw</b> <u>Kuwait</u>
	<b>.it</b> <u>Italy</u>		<b>.ky</b> <u>Cayman Islands</u>
			<b>.kz</b> <u>Kazakhstan</u>

---

<b>.la</b> <u>Lao People's Democratic Republic</u>	<b>.ma</b> <u>Morocco</u>	<b>.na</b> <u>Namibia</u>	<b>.om</b> <u>Oman</u>
<b>.lb</b> <u>Lebanon</u>	<b>.mc</b> <u>Monaco</u>	<b>.nc</b> <u>New Caledonia</u>	
<b>.lc</b> <u>Saint Lucia</u>	<b>.md</b> <u>Moldova</u>	<b>.ne</b> <u>Niger</u>	
<b>.li</b> <u>Liechtenstein</u>	<b>.mg</b> <u>Madagascar</u>	<b>.nf</b> <u>Norfolk Island</u>	
<b>.lk</b> <u>Sri Lanka</u>	<b>.mh</b> <u>Marshall Islands</u>	<b>.ng</b> <u>Nigeria</u>	
<b>.lr</b> <u>Liberia</u>	<b>.mk</b> <u>Macedonia</u>	<b>.ni</b> <u>Nicaragua</u>	
<b>.ls</b> <u>Lesotho</u>	<b>.ml</b> <u>Mali</u>	<b>.nl</b> <u>The Netherlands</u>	
<b>.lt</b> <u>Lithuania</u>	<b>.mm</b> <u>Myanmar</u>	<b>.no</b> <u>Norway</u>	
<b>.lu</b> <u>Luxembourg</u>	<b>.mn</b> <u>Mongolia</u>	<b>.np</b> <u>Nepal</u>	
<b>.lv</b> <u>Latvia</u>	<b>.mo</b> <u>Macau</u>	<b>.nr</b> <u>Nauru</u>	
<b>.ly</b> <u>Libyan Arab Jamahiriya</u>	<b>.mp</b> <u>Northern Mariana Islands</u>	<b>.nt</b> <u>Neutral Zone</u>	
	<b>.mq</b> <u>Martinique</u>	<b>.nu</b> <u>Niue</u>	
	<b>.mr</b> <u>Mauritania</u>	<b>.nz</b> <u>New Zealand</u>	
	<b>.ms</b> <u>Montserrat</u>		
	<b>.mt</b> <u>Malta</u>		
	<b>.mu</b> <u>Mauritius</u>		
	<b>.mv</b> <u>Maldives</u>		
	<b>.mw</b> <u>Malawi</u>		
	<b>.mx</b> <u>Mexico</u>		
	<b>.my</b> <u>Malaysia</u>		
	<b>.mz</b> <u>Mozambique</u>		

---

<b>.pa</b> <u>Panama</u>	<b>.qa</b> <u>Qatar</u>	<b>.re</b> <u>Reunion</u>	<b>.sa</b> <u>Saudi Arabia</u>
<b>.pe</b> <u>Peru</u>		<b>.ro</b> <u>Romania</u>	<b>.sb</b> <u>Solomon Islands</u>
<b>.pf</b> <u>French Polynesia</u>		<b>.ru</b> <u>Russia</u>	<b>.sc</b> <u>Seychelles</u>
<b>.pg</b> <u>Papua New Guinea</u>		<b>.rw</b> <u>Rwanda</u>	<b>.sd</b> <u>Sudan</u>
<b>.ph</b> <u>Philippines</u>			<b>.se</b> <u>Sweden</u>
<b>.pk</b> <u>Pakistan</u>			<b>.sg</b> <u>Singapore</u>
<b>.pl</b> <u>Poland</u>			<b>.sh</b> <u>St. Helena</u>
<b>.pm</b> <u>St. Pierre and Miquelon</u>			<b>.si</b> <u>Slovenia</u>
			<b>.sj</b>

## INTERNET - Möglichkeiten und Dienste

<a href="#">.pn</a> <a href="#">Pitcairn</a>	<a href="#">Svalbard and Jan</a>
<a href="#">.pr</a> <a href="#">Puerto Rico</a>	<a href="#">Mayen Islands</a>
<a href="#">.ps</a> <a href="#">Palestine</a>	<a href="#">.sk</a> <a href="#">Slovakia</a>
<a href="#">.pt</a> <a href="#">Portugal</a>	<a href="#">.sl</a> <a href="#">Sierra Leone</a>
<a href="#">.pw</a> <a href="#">Palau</a>	<a href="#">.sm</a> <a href="#">San Marino</a>
<a href="#">.py</a> <a href="#">Paraguay</a>	<a href="#">.sn</a> <a href="#">Senegal</a>
	<a href="#">.so</a> <a href="#">Somalia</a>
	<a href="#">.sr</a> <a href="#">Surinam</a>
	<a href="#">.st</a> <a href="#">Sao Tome and</a>
	<a href="#">Principe</a>
	<a href="#">.su</a> <a href="#">USSR (former)</a>
	<a href="#">.sv</a> <a href="#">El Salvador</a>
	<a href="#">.sy</a> <a href="#">Syrian Arab Republic</a>
	<a href="#">.sz</a> <a href="#">Swaziland</a>

---


<a href="#">.tc</a> <a href="#">The Turks &amp;</a>	<a href="#">.ua</a> <a href="#">Ukraine</a>	<a href="#">.va</a> <a href="#">Holy See (Vat</a>	<a href="#">.wf</a> <a href="#">Wallis and Futuna</a>
<a href="#">Caicos Islands</a>	<a href="#">.ug</a> <a href="#">Uganda</a>	<a href="#">City State)</a>	<a href="#">Islands</a>
<a href="#">.td</a> <a href="#">Chad</a>	<a href="#">.uk</a> <a href="#">United Kingdom</a>	<a href="#">.vc</a> <a href="#">Saint Vincend the</a>	<a href="#">.wg</a> <a href="#">Western Jordan and</a>
<a href="#">.tf</a> <a href="#">French Southern</a>	<a href="#">.um</a> <a href="#">United States</a>	<a href="#">Grenadines</a>	<a href="#">Gaza</a>
<a href="#">Territories</a>	<a href="#">Minor Outlying</a>	<a href="#">.ve</a> <a href="#">Venezuela</a>	<a href="#">.ws</a> <a href="#">Samoa</a>
<a href="#">.tg</a> <a href="#">Togo</a>	<a href="#">Islands</a>	<a href="#">.vg</a> <a href="#">Virgin Islands</a>	
<a href="#">.th</a> <a href="#">Thailand</a>	<a href="#">.us</a> <a href="#">United States</a>	<a href="#">British</a>	
<a href="#">.tj</a> <a href="#">Tajikistan</a>	<a href="#">.uy</a> <a href="#">Uruguay</a>	<a href="#">.vi</a> <a href="#">Virgin Islands</a>	
<a href="#">.tk</a> <a href="#">Tokelau</a>	<a href="#">.uz</a> <a href="#">Uzbekistan</a>	<a href="#">U.S</a>	
<a href="#">.tm</a> <a href="#">Turkmenistan</a>		<a href="#">.vn</a> <a href="#">Vietnam</a>	
<a href="#">.tn</a> <a href="#">Tunisia</a>		<a href="#">.vu</a> <a href="#">Vanuatu</a>	
<a href="#">.to</a> <a href="#">Tonga</a>			
<a href="#">.tp</a> <a href="#">East Timor</a>			
<a href="#">.tr</a> <a href="#">Turkey</a>			
<a href="#">.tt</a> <a href="#">Trinidad and</a>			
<a href="#">Tobago</a>			
<a href="#">.tv</a> <a href="#">Tuvalu</a>			
<a href="#">.tw</a> <a href="#">Taiwan</a>			
<a href="#">.tz</a> <a href="#">Tanzania</a>			

---

<a href="#">.ye</a> <a href="#">Yemen</a>	<a href="#">.za</a> <a href="#">South Africa</a>
<a href="#">.yt</a> <a href="#">Mayotte</a>	<a href="#">.zm</a> <a href="#">Zambia</a>
<a href="#">.yu</a> <a href="#">Yugoslavia</a>	<a href="#">.zr</a> <a href="#">Zaire</a>
	<a href="#">.zw</a> <a href="#">Zimbabwe</a>

## **Bericht der Bundesregierung**

über die Erfahrungen und Entwicklungen bei den neuen Informations- und Kommunikationsdiensten im Zusammenhang mit der

Umsetzung des Informations- und Kommunikationsdienste-Gesetzes (IuKDG)  [Zum Inhaltsverzeichnis](#)

Copyright © Prof. Jürgen Plate, Fachhochschule München



## **INTERNET - Möglichkeiten und Dienste**

*Prof. Jürgen Plate*

---

# Kleiner E-Mail-Knigge

## Allgemeines

So wie man im Geschäftsleben den "DIN-Brief" oder ähnliche Standardisierungen kennt, so gibt es auch für E-Mails einige Grundregeln. Niemand wird mal eben einen dahingeschluderten Brief abschicken, denn das würde dem Image schaden. Erstaunlicherweise sind viele bei E-Mail nicht so sensibel. E-Mails tendieren zwar dazu, etwas salopper formuliert zu werden als Papierkommunikation, aber sollte es nicht auch bei E-Mails eine gewisse Schmerzgrenze geben? Bedenken Sie dabei, welchen Eindruck Ihr virtueller Gegenüber von Ihnen bekommt.

Wenn man also jemandem etwas mitteilen will, sollte man dafür sorgen, daß der Empfänger das auch lesen kann. Dies geht über die bloße Möglichkeit, den Text zu entziffern, hinaus. Ein gut lesbarer Text wird wesentlich mehr Aufmerksamkeit erfahren. Auch will sich sicher niemand als jemand outen, der von elementaren Grundregeln der elektronischen Kommunikation keine Ahnung hat. In den vergangenen mehr als 25 Jahren haben sich Regeln für das E-Mail-Schreiben herausgebildet, die von jedem erfahrenen Internet-Nutzer eingehalten werden:

- **Die Wahl des Subjects (Betreff).** Hier achte man auf Aussagekraft. Da viele Mail-Programme eine Übersichtsliste der E-Mails mit begrenzter Länge darstellen, sollte sich der Inhalt vor allem am Anfang des Subjects finden. Lange Subjects sollte man vermeiden, da einige Programme dabei Probleme haben (z.B. fügt Netscape unmotiviert Leerzeichen ein).
- **Realname.** Der Realname ist der wirkliche Name des Absenders (also Vor- und Nachname). Er sollte auf jeden Fall in der From-Zeile stehen. Das muß man in der Konfiguration des Mail-Programms erledigen.
- **Unterteilung in Absätze.** Texte lesen sich besser, wenn sich das Auge an optischen Marken festhalten kann. Endlose Absätze sind einfach schlecht lesbar. Man trenne Absätze durch Leerzeilen.
- **Zeilenlänge und Umbrüche.** Eigene Texte sollte man auf etwa 70 Zeichen pro Zeile umbrechen (die meisten Mail-Programme machen das auf Wunsch automatisch). Längere Zeilen sind schlecht lesbar und führen oftmals beim Zitieren (Quoten) zu Problemen. Wörter mittels Bindestrich zu trennen, ist unüblich und beim Umformatieren von Zitaten ausgesprochen lästig; dies sollte man nur in extremen Ausnahmefällen machen, etwa wenn sonst halbleere Zeilen resultieren würden.
- **Zeichensätze.** Standard ist ASCII; kurz gesagt ist das alles, was man braucht, um einen englischen Text zu schreiben, es fehlen also insbesondere die Umlaute diverser Sprachen. Der nächste gängige Zeichensatz ist ISO-8859-1 (auch "latin1" genannt). Neuer ist ISO-8859-15, der sich von vorgenanntem vor allem durch das Euro-Zeichen unterscheidet. Verwenden sollte man nur Zeichen, die das Mail-Programm des Empfängers richtig dekodieren kann. Mit ASCII kann jeder umgehen. Mit ISO kommt eigentlich auch jeder klar. Nach Möglichkeit vermeiden sollte man Nicht-ASCII-Zeichen im Header und im Subject. Einfacher Text mit einer nicht-proportionalen Schriftart (alle Zeichen sind gleich breit, etwa Courier) hat natürlich nur sehr begrenzte Möglichkeiten, ist aber für E-Mail zweckmäßig; nur mit derartigen Schriften ist es möglich, Effekte wie Unterstreichungen oder "Tabellen" so zu schreiben, daß alle sie lesen können.
- **Signatures.** Hier kann man am Ende einer Mail (typischerweise automatisiert) noch ein paar Zeilen mit Informationen, witzigen Sprüchen o.ä. anfügen. In RFC-1855 heißt es aber, daß eine Signature (oder nennen wir's Visitenkarte) maximal vier Zeilen lang sein sollte. **Zur Trennung vom Text fügt man vor der Signatur eine Zeile ein, die zwei Minus- und ein Leerzeichen (also "-- "; in genau dieser Reihenfolge) und nichts anderes enthält.** Das Leerzeichen ist wichtig! Ordentliche Mail-Programme können dann die Signatur automatisch abtrennen. Daß man auch in fünf Zeilen etwas sagen kann, zeigt folgendes Beispiel:

--

## INTERNET - Möglichkeiten und Dienste

```
(_) == Prof. Juergen Plate == (_)  
~~\-----(..) == Fachhochschule Muenchen, FK 04 == (oo)-----\  
* || (__) == Lothstrasse 64, 80335 Muenchen == (__) || |  
* ||w--|| == Telefon +49-(0)89-1265-0 == ||--w|| ~
```

Wer unbedingt noch weitere Informationen unterbringen will, kann z. B. konform zum Standard, das "Organisation"-Feld des Mail-Headers ausfüllen. Das geht beispielsweise mit Netscape folgendermaßen.

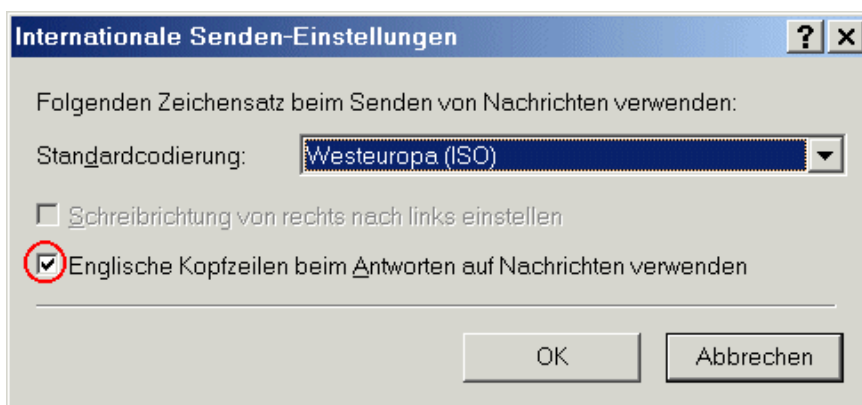
Unter *Edit -> Mail and Newsaccount-Settings* auf den obersten Eintrag klicken (der sollte die Absenderadresse enthalten) und dort unter *Organisation* den Namen der Firma oder Hochschule eintragen. Das wird dann sauber im Kopf jeder Mail vermerkt. Deshalb hat auch die Absender-E-Mail-Adresse nichts in der Signature zu suchen (steht ja schon im Header).

Von allzu vielen Informationen in einer E-Mail (Web- oder Post-Adressen sowie Telefonnummern) ist eher abzuraten. Man weiß nie, in welche Hände E-Mails fallen; inzwischen gibt es schon etliche Roboterprogramme, welche Webadressen, E-Mailadressen und Telefonnummern aus den Signatures extrahieren und diese Daten dann Werbefirmen anbieten; frei nach dem Motto "30000 Telefonnummern aus deutschen Firmen".

- **Großgeschriebene Wörter** werden von der überwiegenden Mehrheit als Schreien 'gehört'. Es mag in der E-Mail zwar Teile geben, bei denen es nötig ist, zu Schreien, ABER SELTEN DIE GANZE E-MAIL LANG! Schreien Sie die Leute nicht an. Es ist unhöflich.

Die sogenannten "V-Cards" und ähnlicher Tüddelkram blasen die E-Mail nur unnötig auf und haben keinen praktischen Nutzwert. Kennt man den Empfänger nicht, sollte man auch mit Informationen sparsam sein (siehe auch bei "Signatures"). Kennt man sich oder hat man öfter miteinander zu tun, genügt der einmalige Austausch von Adresse und Telefonnummer - das muß dann nicht an jede E-Mail angehängt werden.

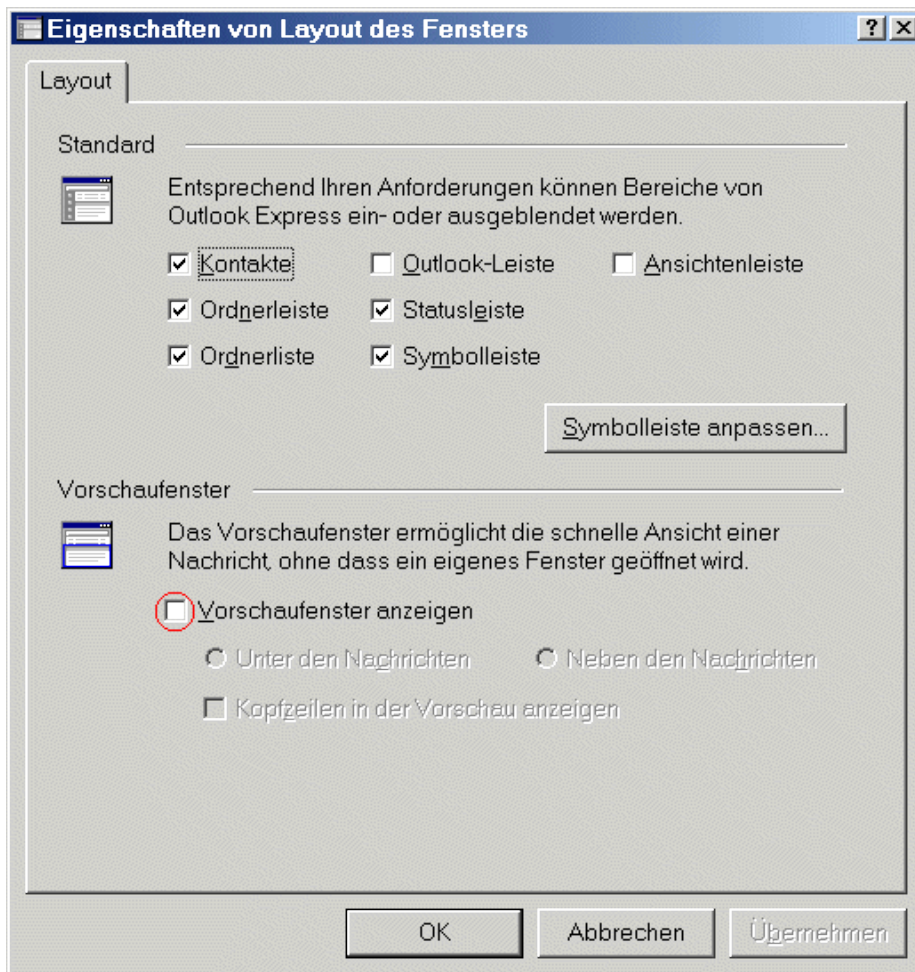
- **Überprüfung der Einstellungen des Mail-Programms.** Am Anfang oder nach Wechsel der Mailsoftware sollte man überprüfen, daß die eigene E-Mail dem entspricht, was hier beschrieben ist. Dazu schickt man sich selbst eine E-Mail, die möglichst viele der hier aufgeführten Punkte erkennen läßt. Insbesondere sollte man sein Programm konform zu den Standards machen (RFC-Dokumente). Bei Outlook kann dies durch ein kleines Häkchen im Einstellungsmenü geschehen. Klicken Sie unter *Extras - Optionen* auf dem Reiter *E-Mail-Format* auf dem Knopf *internationale Optionen* und wählen Sie im Pop-Up-Menü den Punkt "Kopfzeilen von Antworten und Weiterleitungen in Englisch" aus. Dann können Sie auch gleich noch unter "Codierung für ausgehende Nachrichten" den Punkt "Westeuropa(ISO)" auswählen. Bei Outlook Express findet sich der Knopf "Internationale Einstellungen" auf dem Reiter "Senden" des Optionen-Dialogs.



Gleich noch ein Hinweis: Bei Outlook Express sehen Sie sofort die E-Mail in einem Vorschauenfenster, sobald Sie auf eine Nachricht im Posteingang klicken. Manche Viren werden schon durch diese Vorschau aktiviert. Daher sollten Sie das Vorschauenfenster abschalten. Die

## INTERNET - Möglichkeiten und Dienste

Einstellung dazu ist aber nicht leicht zu finden. Sie versteckt sich unter *Ansicht - Layout*. Im folgenden Dialog deaktivieren Sie das Kontrollkästchen "Vorschauenfenster anzeigen". Bestätigen Sie die Änderungen nacheinander mit "Übernehmen" und "OK".



### Regeln für Antwortmails (Zitieren)

Am Anfang sollte man vor allem sagen, auf wen man sich bezieht. Weitere Angaben sind fast immer überflüssig, da sie im Header ablesbar sind (z.B. Subject der Bezugsnachricht, Message-ID der Bezugsnachricht (bei den meisten Programmen)). Diese Einleitungszeile sollte man kurz halten, maximal zwei Zeilen reichen. Lange "witzige" Einleitungen langweilen schnell. Selbiges gilt erfahrungsgemäß auch für Anreden etc.

- **Zitieren** Das Zitieren der vorangegangenen Mail erfolgt durch Voranstellen des Größer-Zeichens an jedem Zeilenanfang. Das macht in der Regel das Mail-Programm automatisch. Wichtig ist dabei, daß die zitierten Zeilen **keinesfalls** umbrochen werden. Hiervon ausgenommen sind natürlich händische Eingriffe, um den Text zu trennen oder besser lesbar zu machen.

Wichtig ist die Frage, wie viel man denn nun zitieren soll. Die Antwort ist einfach: So viel, wie für das Verständnis der Antwort nützlich oder notwendig ist, so wenig wie möglich! Das heißt insbesondere, daß man all das, auf das man nicht eingeht, komplett löscht. Möchte man eine längere Passage des Vorredners zusammenfassen, so schreibt man in eine einzelne Zeile in eckigen Klammern ein/zwei Stichworte hin und löscht dafür den betreffenden Abschnitt. Zwischen Zitaten und den eigenen Texten, die man dort zwischen die Zitaten schreibt (jeweils **unter** die Bezugsstelle), wo sie inhaltlich hingehören, fügt man zur optischen Trennung eine Leerzeile ein.

Die normale Leserichtung ist von links nach rechts und von oben nach unten, und man

## INTERNET - Möglichkeiten und Dienste

erwartet in dieser Richtung auch eine zeitliche und logische Abfolge in den Texten, die man liest. Vor allem Leser, die eine Menge von E-Mails lesen (und damit, nebenbei bemerkt, ideale Antwortgeber sind), schätzen es sehr, wenn sie zuerst den Text lesen können, auf den man sich bezieht. Das Zitat dient hier als Erinnerungshilfe, die natürlich dann nicht gegeben ist, wenn das Zitat am Ende steht.

Außerdem ist es hierzulande so üblich. Das mag ein schwaches Argument sein. Aber mal ehrlich: ist man nicht verwundert, wenn man erst die Antwort erhält und dann die Frage gestellt bekommt?

Es sollte klar sein, daß es ein Kardinalfehler ist, "Vollquotes", noch dazu am Ende der Mail (sogenanntes *TOFU* = Text Oben Fullquote Unten), einzufügen. Das will keiner mehr lesen. Leute, die so etwas tun, nennt man *Vollquottel*.

- **Subject verändern.** Gelegentlich möchte man bereits im Subject kennzeichnen, daß sich das Thema verschoben hat, dann ändert man das Subject. Ständige Änderungen ohne wirklichen Grund oder gar, um dort schlagwortartig eine Aussage zu plazieren, sind schlechter Stil.
- **Re:** Antworten - *und nur solche* - tragen am Anfang des Subjects die Zeichenkette "Re:" plus Leerzeichen. Jegliche andere Kennung ist von Übel und kann von den meisten Programmen nicht richtig erkannt werden (außerdem ist es nicht Standard-Konform). Auch bei Outlook läßt sich das einstellen!

## Attachments

Anhänge (Attachments) sind meist lästig, wenn nicht klar ist, daß der Empfänger genau weiß, was er damit soll, was vor allem bei proprietären Datenformen (z.B. Word-Dateien, vcard) schwierig sein kann. HTML verbietet sich aus denselben Gründen (und hat noch dazu in fast allen Fällen keinen Mehrwert). Office-Benutzer glauben immer, ihre Dokumente im jeweiligen Format per E-Mail weitergeben zu müssen. Natürlich kann man jegliche Dateien als Anhang einer E-Mail (sogenanntes Attachment) verschicken - was mitunter auch sinnvoll ist. Nur sollte man dabei immer auch an den Empfänger denken, denn nicht immer ist ein Attachment notwendig oder sinnvoll. Für alle Attachments gilt: Wer solche Dateien erhält, muss natürlich auch das passende Programm zur Darstellung der Inhalte besitzen. Teilweise kann ein Attachment auch Gefahren bergen. Office-Dokumente können Makroviren enthalten. Daher sind viele Empfänger heute sensibilisiert (siehe unten Viren, Phishing) und eher Abgeneigt solche Dateien zu öffnen. Aber auch "harmlose" Makros können beim Empfänger nicht gewünschte Effekte hervorrufen. Hinzu kommt, daß der Empfänger möglichst auch die passende Office-Version besitzen muß, um das Dokument zu öffnen.

Eine weitere Gefahr ist das ungewollte Preisgeben von Daten. Office-Dokumente enthalten Daten über den Autor, das Erstellungsdatum, den Dateipfad, den Makropuffer, den Löschpuffer (Stichwort: Änderungen verfolgen) und vielleicht noch mehr. Es gab einmal den Fall einer Powerpoint-Präsentation mit einer Preisliste darin. Die Präsentation zeigte zwar nur die Verkaufspreise der eingebundenen Excel-Tabelle. Nach Herauslösen der Tabelle war aber die Spalte "Einkaufspreis" wieder sichtbar. Mitunter werden sogar Fonts ins Dokument eingebunden. Die (unwissentliche) Weitergabe von Fonts kann sogar zu Copyright-Konflikten und damit vor den Kadi führen.

In etlichen Fällen ist es auch nicht nötig einen schön formatierten Text weiterzugeben. Gerade bei E-Mails reicht meist einfacher Text. Oft geschieht das Anhängen eines Dokuments nur aus Faulheit (statt den Inhalt mit Cut-and-paste zu übernehmen. Soll aber soch ein "schönes" Dokument versendet werden, bieten sich die Formate PDF, HTML, XML, LaTeX oder RTF an.

## Legenden und Hoaxes

Legenden sind recht unterhaltsam, wenn sie das erste Mal auftauchen; verzeihbar auch noch beim zweiten Mal, aber nicht mehr, wenn's das siebte Mal ist, wenn es sie schon seit Monaten oder Jahren

gibt. (Beispiel: Kostenlose Mobiltelefone von 'bitte passende Firma einsetzen', der arme Craig Shergold, der gerne eine Visitenkarte möchte oder die Virenwarnung, die man an alle Freunde und Bekannten verschicken soll). Diese Geschichten leben weiter, weil es offensichtlich Menschen gibt, die denken, daß Sie für jedermann neu sein müssen, weil sie doch jetzt erst davon gehört haben. Wenn man sich die vielen Webseiten über Legenden und Hoaxes ansieht, ist es eine Schande, daß viele bereit sind, ihre Glaubwürdigkeit zu ruinieren, indem sie an solche Geschichten glauben. Man muß davon ausgehen, daß die Absender die Geschichten glauben, weil sie diesen Müll verschicken, ohne daß sie nachgedacht oder vorher einmal die einschlägigen Webseiten gelesen haben.

### E-Mail-Viren und SPAM

Neulinge im Netz werden öfters erschreckt durch die Meldung, daß man keinesfalls eine E-Mail mit dem Betreff "Good Times" (oder auch einem anderen Subject) lesen soll, da sonst ein Virusprogramm auf den Rechner gelangt. Das stimmt natürlich nicht. Durch alleiniges Lesen einer E-Mail kann meist nichts passieren. Leider sind einige Betriebssysteme und E-Mail-Programme inzwischen so angreifbar geworden, daß schon beim Öffnen der E-Mail ein in der Mail enthaltener Programmcode zur Ausführung gelangt. Da hilft es nur, auf andere Programme auszuweichen. Anders verhält es sich, wenn diese E-Mail eine angehängte Datei ("Attachment") mit sich führt. Diese Datei kann sehr wohl Gefahren mit sich bringen:

- Wenn es sich um eine ausführbares Programm handelt, besteht die Möglichkeit, daß dieses Programm Viren enthält - nicht anders, als wenn Sie das Programm auf Diskette erhalten hätten.
- Bei Winword-Dokumenten können sich im Dokument sogenannte "Makroviren" verbergen. Das sind Word-Makros mit schädlichen Funktionen, die gegebenenfalls automatisch aktiviert werden, wenn Sie das Dokument mit Winword öffnen.  
Zu dieser Gruppe gehört z. B. auch das Melissa-Virus, das sich die Adressdatenbank von Outlook schnappt und sich selbst an alle dort aufgeführten Adressen schickt. Da nun Sie als Absender in den Mails stehen, bekommen Sie wohlmöglich auch noch den Zorn der Empfänger ab. Melissa war erkennbar durch den Registry-Eintrag  
"HKEY\_CURRENT\_USER\Software\Microsoft\Office\Melissa?".  
Melissa und ähnliche Viren führen dazu, daß man nicht nur Mails von unbekanntem Absendern mißtrauen muß, sondern auch solchen von Bekannten.  
Ähnliches gilt auch für andere Anwendung mit Skriptsprache, z. B. Excel. Die Problematik bei Microsoft besteht unter anderem darin, daß beispielsweise der Internet-Explorer andere Microsoft-Applikationen grundsätzlich als vertrauenswürdig betrachtet und daher auch keine Warnung erfolgt.
- Dateien im PDF-Format können auch gefährliche Inhalte haben. Der Acrobat-Reader zum Betrachten der Dokumente kann auch beliebige Kommandos auf dem PC starten. Diese Kommandos können sich hinter harmlosen Buttons verbergen (z. B. "Zurück zum Inhalt").

Es gibt noch ein paar andere Sorten von E-Mail, die zwar nicht gefährlich, aber doch lästig sind. Wie bei der Briefpost kommen mit der Zeit auch Werbe-E-Mails, welche die Mailbox verstopfen. Die zweite Sorte sind Kettenbriefe wie man sie auch seit vielen Jahren kennt. Meist tragen sie ein Subject der Art "MAKE MONEY FAST". Schließlich geistern seit jahrzehnten herzerweichende E-Mails durch das Netz, die von einem krebserkrankten Jungen erzählen (z. B. Craig Shergold), der gerne noch ins Guinness-Buch der Rekorde kommen möchte und dem man deshalb eine Postkarte oder Visitenkarte schicken soll. Tun Sie das nicht, denn entweder ist der Kleine schon 30 - 40 Jahre alt oder längst verstorben.

### Wie war das mit "I Love You"?

- Eine Textdatei mit einigen wenigen Ablaufbefehlen für die Programmiersprache Visual Basic erschütterte nachhaltig das Vertrauen in die E-Mail als Kommunikationsmittel. Die

## INTERNET - Möglichkeiten und Dienste

verhängnisvolle Botschaft war dabei Virus, Wurm und Trojanisches Pferd in einem.

- Das **Virus** des "I Love You"-Briefes löschte Bild- und Tondateien in den Formaten .jpg und .mp3 und verbarg Videodateien im MPEG-Format. Aber nur bei Menschen, die ein bestimmtes E-Mail-Programm von Microsoft benutzten.
- Das **Trojanische Pferd** des "I Love You"-Briefes versuchte, eine Web-Seite aufzurufen und von ihr die Datei `winbugsfix.exe` ins heimische System zu kopieren. Das war ein Programm, das Passworteingaben und andere Einstellungen des Internet Connection Wizard von Microsoft sowie alle Internet-Adressen interner Server an einen Empfänger auf den Philippinen schicken wollte.
- Der **Wurm** im "I Love You"-Brief schickte über die E-Mail-Software Microsoft Outlook an jeden Eintrag im Adressbuch eine Kopie seiner selbst. Ein anderer Teil des Skriptes hatte es auf die privaten Besucher von Chatforen abgesehen. Jeder, die die Chatsoftware mIRC benutze, bekam automatisch auch den "I love You"-Brief.

Zeitungen und Multimedia-Firmen verloren ihre Bild-Datenbanken. Warum? Gab es keine Datensicherung? Kein Backup? Tatsächlich dokumentiert die schnelle Verbreitung des "I Love You"-Virus ein derartiges Maß an fehlendem Sicherheitsbewußtsein selbst in großen Firmen und Institutionen, dass die Experten nachgerade verzweifeln.

Die Links innerhalb des Scripts offenbaren drei Pseudonyme von Usern, zum Beispiel:

`http://www.skyinet.net/~koichi`. Auf deren Homepage lag das Programm, das "I Love You" zur Datenspionage verwenden wollte. Seinen Provider verrät uns zum Beispiel die Datenbank Allwhois. Man muß nur `skyinet.net` in das Suchfenster eingeben und erhält Namen, Adresse und Telefonnummer: Sky Internet, Inc., L/G Victoria I Bldg. 1670 Quezon Ave, Quezon, Ph 1103 8000, +63 2 411-2005. So kommt man auch sicher an deren Kunden mit dem Pseudonym "koichi".

### Was kommt sonst noch mit der E-Mail

Die meisten Mail-Programme werfen sofort den Web-Browser an, wenn sich HTML-codierter Text in der E-Mail befindet. Leider ist es eine Unsitte, dass viele Programme als Voreinstellung den Versand von HTML-codierten Dokumenten haben. Damit kann man sich neben den oben genannten Viren auch beispielsweise das folgende einhandeln (original so bei mir eingetroffen):

```
<BODY>
<P><FONT Color="#100001" FACE="Verdana" SIZE="2">
<B>Hey Du</B><BR><BR>
Am besten sofort anrufen:
<BR>
<B>Tel 0067.710.523
</B><BR>
Total affig!
<BR><BR>
EineÜberraschung von ??
</FONT>

</P></BODY>
```

Sobald die E-Mail geöffnet wird, ruft der Bilder-Link (`<img src=...`) ein Programm namen `RpC.ddd` auf und gibt ihm die beiden Werte von `a` (`plate@fhm.edu`) und `b` (`0067SS`) mit. Damit weiß das System des Spammers nicht nur, daß die E-Mail-Adresse gültig ist, sondern sogar wann und von welchem Rechner (IP-Nummer) aus die E-Mail gelesen wurde.

Wer wissen will, wie intelligent E-Mail-Viren heute sind, der kann sich die vier Artikel bei Heise Security durchlesen. Sie sind nicht nur echt witzig geschrieben, sondern auch echt interessant:

<http://www.heise.de/security/artikel/59611>

## Was ist eigentlich Spam? Und was bedeutet ECP, EMP, UBE, UCE?

Zunächst eine knappe Erläuterung der Abkürzungen:

- *Spam*: Belästigende Massennachricht (Mail und News)
- *ECP*: Massen-Crossposting (News)
- *EMP*: Massenposting aus vielen identischen Einzelpostings bestehend (News)

Wird ein Artikel gleichlautend in übermäßig viele Newsgroups gepostet oder crosspostet, so spricht man im ersten Falle von Spam oder EMP (excessive multiple posting), im zweiten von Velveeta bzw. ECP (excessive cross-posting).

SPAM steht für "Spiced Pork and hAM(\*)", so eine Art Preßfleisch, das in Amerika verkauft wird (sieht aus wie Katzenfutter). Es gibt einen Sketch aus Monty Python's Flying Circus, in dem ein Paar in einem Restaurant die Speisekarte vom Kellner vorgelesen bekommt und in jedem Gericht ist SPAM drin, zum Teil sogar mehrfach. Auch in dem Restaurant sitzt eine Gruppe Wikinger, die am Ende des Sketches 'Lovely Spam, wonderful Spam!' singen. Insgesamt kommt in dem Sketch das Wort SPAM ca. 120 mal vor.

(\*) Manche Leute behaupten, es steht für Synthetically Produced Artificial Meat.

Bei E-Mail spricht man von:

- *UBE*: Unerwünschte Massennachricht (unsolicited bulk E-Mail)
- *UCE*: Unerwünschte Werbenachricht (unsolicited commercial E-Mail)

Da UCE zunehmend lästiger wird, sind in letzter Zeit einige Leute auf die Idee gekommen, ihre News-Artikel unter einer falschen Adresse zu posten. Im Body des Artikels finden sich dann meistens Hinweise auf eine gültige Adresse. Diese Methode, sich gegen UCE zu wehren, ist jedoch problematisch. Wird der Domain-Teil der Adresse verändert, kann es passieren, daß diese Adresse trotzdem gültig ist (sogar 'xxx.de', 'nospam.de' oder 'deletethis.de' sind beim DE-NIC registriert. Wird nur der Namens-Teil der Adresse verändert, erhält zumindest der Postmaster einer Fehlermeldung per Mail. Die UCE-Versender bekommen von Fehlermeldungen/Bounces dagegen in der Regel nichts mit, da sie fast nie unter einer gültigen E-Mail-Adresse ihre UCE versenden bzw. keine gültige Rücksendeadresse angegeben haben.

Sinnvoller ist es deshalb, das Problem UCE an der Wurzel zu packen. Dies kann durch das Einrichten von Teergruben oder durch das Filtern von bekannten Spammer-Domains geschehen.

- Spammer wollen mit einfachsten Mitteln Geld verdienen!  
Entweder locken Spammer ihre Opfer mit SPAM-Methoden auf Webseiten, um dort ein bestimmtes Produkt zu verkaufen (z.B. über einen Link zu einem kostenpflichtigen Porno-Angebot oder zu den gefürchteten *0190-Dialern*). Oder sie versuchen, eine Website bekannt zu machen, die sich über Werbung finanziert, und auf möglichst viele Besucher angewiesen ist.
- Spammer versuchen ihren Empfängern zu schaden  
Manchmal versuchen Spammer einfach nur, möglichst viel Datenverkehr zu erzeugen, um E-Mail-Server lahmzulegen, und die Ressourcen von Konkurrenten zu verschwenden. Rechtlich gesehen ist das Versenden von SPAM in den EU-Staaten eine kriminelle Handlung! Die augenblickliche Gesetzeslage sieht zwar theoretisch einen rechtlichen Schutz für die Opfer vor, jedoch dürfte es praktisch äusserst schwierig sein, Spammern bis in die rechtsfreien Untiefen des Internets zu folgen... (in der Regel versuchen Spammer mit effektiven Mittel ihre Herkunft zu verschleiern...)

### Die Tricks der Spammer

Um Ihre Opfer zu erreichen, brauchen die Spammer zuerst eine gültige E-Mail-Adresse, an die sie auf verschiedenen Wegen gelangen:

- Der E-Mail Anbieter (z.B. ein Anbieter kostenloser E-Mail-Zugänge) verkauft die E-Mail-Adressen der Kunden weiter. Selbst wenn der E-Mail-Anbieter im Grunde seriös ist, kann es sein, dass er die E-Mail-Adresse des Opfers an einen vermeintlich seriösen Werbekunden weiterverkauft, dieser die Adressen verwendet aber zusätzlich an unseriöse Anbieter weiterverkauft.
- Der Spammer findet die E-Mail-Adresse über spezielle Suchmaschinen, die das Internet systematisch nach E-Mail-Adressen durchsuchen.
- Durch Ausprobieren: Der Spammer spielt alle möglichen Empfängernamen bei einer Domain durch.

Wenn der Spammer systematisch gebräuchliche Namen aus einem Wörterbuch vor die Domainnamen größerer Websites setzt, z.B. john@gmx.de, meier@firma.de, usw., ist die Wahrscheinlichkeit ziemlich groß, dass er mit einem Teil dieser Mails einen Empfänger erreicht.

Wenn die Mail an einen ungültigen Empfänger gerichtet ist, wird gewöhnlich eine Fehlermeldung an den Absender (in diesem Fall den Spammer) zurückgeschickt, und der Spammer kann die nächste Möglichkeit ausprobieren. Wenn die Mail einen gültigen Empfänger erreicht, und keine Fehlermeldung zurückkommt, weiß der Spammer, dass die Adresse existiert, und speichert diese in seiner "Opfer-Datenbank"

In der Regel wird der Spammer aber versuchen seine Absenderadresse zu verschleiern, bzw. einfach eine ungültige Absenderadresse anzugeben, so dass er auf direktem Weg keine Antwort erhalten kann. Um trotzdem eine Bestätigung über die Existenz des Opfers zu erhalten, benutzt er einen einfachen Trick:

Er merkt sich einfach zu jeder versendeten E-Mail einen systematisch erzeugten Schlüssel, z.B. eine lange Zufallszahl. Diese Zahl wird in einen gewöhnlichen Hyperlink eingebaut, z.B:

...

Um sich aus dieser Mailingliste wieder auszutragen klicken Sie auf:

<http://www.firma.de/reply.cgi?id=2374654000332>

Wenn der naive Empfänger jetzt auf diesen Link klickt, oder die Nachricht zurückschickt, braucht das Programm auf dem Webserver nur noch den übergebenen Schlüssel mit den gemerkten Schlüsseln zu vergleichen, und kennt wieder eine gültige Opferadresse mehr.

Doch selbst, wenn man nicht auf die Links in der SPAM-Mail klickt, kann er Spammer z.B. bei HTML-Mails den Link als externe Ressource verlinken (Bilder, Töne, Flash). Die E-Mail enthält dann einen Hyper-Link in der Art

```

```

Dieser Link wird vom Mail-Programm normalerweise als Link auf ein Bild interpretiert. Es wird daher versuchen, das Bild von der angegebenen Adresse zu laden. Und dort freut sich schon der Webserver des Spammers auf die ID des Besuchers.

Selbstverständlich werden die Netzwerkeffekte des Internets auch von den Spammern genutzt, so dass die Datenbankbestände vieler einzelner Spammer zusammengefasst und auf CDs an andere Spammer weiterverkauft werden (die Angebote für diese CDs werden teilweise als SPAM verschickt).

## Phishing - Passwort-Fischer

Seit Ende 2004 gibt es eine weitere Plage: "Phishing". Das klingt nach "fischen gehen" - und genau so ist es auch. Das Wort setzt sich aus "Password" und "fishing" zusammen, also "angeln nach Passwörtern". Es ist der Oberbegriff für illegale Versuche, Computeranwendern Zugangsdaten (Loginnamen, Passwörter, Kreditkartendaten, Bank-TANs, etc.) zu entlocken. Phishing ist also eine Form des Trickbetruges mit Methoden des Social Engineering. Immer öfter fälschen Phishing-Betrüger E-Mails und Internetseiten, womit sie einen neuen Weg gefunden haben, um an vertrauliche Daten heran zu kommen - die Nutzer geben ihre Daten einfach freiwillig preis.

Gängige Ziele von Phishing-Attacken sind Zugangsdaten für Banken (Onlinebanking), Versandhäuser, Internet-Auktionshäuser, webbasierende Onlineberatungen oder Kontaktportale. Durch den anschließenden Mißbrauch der gestohlenen Zugangsdaten wird den Opfern Schaden zugefügt. Als Bank oder Firma getarnt fordern die Betrüger den Empfänger in der E-Mail auf, seine Daten zu aktualisieren - weil beispielsweise die Kreditkarte ablaufe, das Passwort erneuert werden müsse oder die Zugangsdaten verloren gegangen seien. Der Inhalt der so genannten Phishing-Mails wirkt manchmal erbärmlich dilettantisch, teilweise aber auch täuschend echt. Diese E-Mails im HTML-Format zeigen einen scheinbar "offiziellen" Link an, hinter dem sich jedoch ein Link auf die Webseite des "Phischers" verbirgt. Der Empfänger wird für die Dateneingabe also auf eine Internetseite geführt, die z. B. der Banken-Homepage ähnlich sieht. Auf den ersten Blick scheint alles ganz normal, selbst die Eingabeformulare sehen gleich aus. Folgt er der Aufforderung in der E-Mail, gelangen seine Zugangsdaten in die Hände der Urheber der Phishing-Attacke. Was dann folgt dient nur noch dazu, nachträgliches Mißtrauen des Anwenders zu zerstreuen. Eine kurze Bestätigung oder eine Fehlermeldung. Dann wird das Opfer auf die echte Webseite weitergeschickt. Eine weitere Variante besteht darin, ein Formular direkt innerhalb der E-Mail einzubinden, welches zur Eingabe der Daten auffordert und diese an die Urheber sendet. Auf eine gefälschte Website wird hierbei ganz verzichtet.

Die Phishing-Betrüger nutzen dabei entweder Internetadressen, die sich nur geringfügig von denen der renommierten Firmen unterscheiden. Oder aber sie fälschen die Adressleiste des Browsers mit einem Java-Script. Man glaubt also, man sei auf einer seriösen Seite, ist es aber nicht. Eine Adresszeile der Form `http://192.168.22.33/security/` verrät gleich, daß man sich nicht auf den Seiten einer Bank befindet. Deshalb werden oft Webadressen verwendet, die den originalen Adressen ähneln, z.B. `http://www.login-beispielbank.de/`. Seit Anfang 2005 besteht die Möglichkeit, Umlaute innerhalb von Webadressen zu verwenden. Daraus resultieren auch neue Möglichkeiten der Adress-Namensverfälschung. Lautet beispielsweise die Originaladresse `http://www.koelner-bank.de`, kann der Phischer `http://www.kölnner-bank.de` verwenden. Noch schwerer zu erkennen ist die Verwendung von kyrillischen Buchstaben anstelle von Umlauten. Das kyrillische "a" unterscheidet sich optisch in keiner Weise vom lateinischen "a". Es kann z.B. das "a" in "bank" bei `http://www.beispielbank.de/` kyrillisch dargestellt werden. Diese Methode ist selbst für Experten erst bei genauerem Hinsehen zu durchschauen.

Banken und Versicherungen versenden niemals per E-Mail die Aufforderungen, Zugangsdaten einzugeben. Keinesfalls fragen sie nach Transaktionsnummern oder Transaktionspasswörtern für das Onlinebanking. Sie senden Ihnen bei sicherheitsrelevanten Fragen Briefe und Einschreiben oder man bittet Sie, persönlich in der Filiale vorzusprechen. Folgen Sie deshalb niemals Weblinks aus einer unaufgefordert zugesandten E-Mail. Geben Sie vielmehr die URL zum Onlinebanking immer von Hand in die Adresszeile des Browsers ein oder benutzen Sie im Browser gespeicherte Favoriten/Lesezeichen, die Sie selbst angelegt haben. Meist lassen sich Phishing E-Mails an folgenden Merkmalen erkennen:

- Es geht um eine "Sicherheitsüberprüfung", "Verifikation" oder "Freischaltung". Alles, was wichtig klingt.
- Die Nachricht enthält ein Link.

## INTERNET - Möglichkeiten und Dienste

- Es wird angedroht, bei Nichtbeachtung würde ein Zugang gesperrt oder gelöscht oder sonst etwas Schlimmes.
- Es fehlt die persönliche Anrede. Es gibt nur eine allgemeine Anrede ("Sehr geehrter Kunde", "Sehr geehrtes EBay-Mitglied").
- Rechtschreib- und Grammatikfehler im Text.

Beispiel:

Sehr geehrter Kunde!

Ihr Konto wurde von der Datensicherheitsdienst zufälligerweise zur Kontrolle gewählt. Um Ihre Kontoinformation durchzunehmen, bitten wir, damit Sie uns mit allen Angaben versorgen, die wir brauchen. Sonst koennen wir Sie identifizieren nicht und sollen Ihr Konto fuer seine Verteidigung blockieren. Fuellen Sie bitte das Formular aus, um alle Details Ihres Kontos zu pruefen.

Danken schoen.

## Pharming

Phishing, als Möglichkeit an Passwörter und PINs von unbedachten Usern zu gelangen ist hinreichend bekannt. Nun kristallisiert sich ein neuer Trend beim Abgreifen dieser Daten heraus: Pharming. Pharming ist einfach ein neuer Name für einen relativ alten Angriff, das sogenannte "Domain-Spoofing".

Pharming könnte sich zu einer noch größeren Bedrohung für die Sicherheit im Netz entwickeln als Phishing. Auch beim Pharming wird versucht, Passwörter und Geheimnummern abzugreifen. Selbst ein sorgfältiger Internetnutzer kann Opfer von Pharming-Angriffen werden.

Anders als beim Phishing landet bei einem erfolgreichen Pharming-Angriff selbst ein User, der vorausschauend keinem Link in einer Phishing-Mail folgt und stattdessen die URL per Hand im Browser eingibt, oder die Seite über einen Bookmark aufruft, auf einer falschen Seite. Diese Seite sieht dann zwar wie die originale Seite aus und taucht auch mit dem originalen Namen in der URL-Zeile auf, residiert aber auf dem Server eines Angreifers.

Pharming nutzt die Auflösung von Namen zu IP-Adressen im Internet aus. Wenn ein User eine Adresse (z. B. "www.stadtparkasse.de") eingibt, muss diese URL-Adresse zu einer numerischen Adresse (wie 193.99.144.80) aufgelöst werden, über die dann eine Verbindung aufgebaut werden kann. Diese Namensauflösung führen DNS-Server (DNS = Domain Name System) durch, die dazu Datenbanken von IP-Adressen und Domain-Namen verwalten. Aber auch lokal werden Adresslisten verwaltet, die einem Domain-Namen einer Adresse zuordnen. Bei Windows ist dies die Datei `C:\WINDOWS\system32\drivers\etc\hosts`, bei Linux `/etc/hosts`. Wenn dort eine Zuordnung eingetragen wird, verwendet der Browser (und auch alle anderen Internet-Programme) diese Datei, bevor andere Nameserver abgefragt werden.

Pharming-Betrüger manipulieren die Hosts-Datei so, dass einem bestimmten Domain-Namen eine andere numerische Adresse zugeordnet wird. Der Benutzer landet also auf einer ganz anderen Website auf einem ganz anderen Server, als er denkt. Davon merkt der Benutzer aber nichts, weil die dort hinterlegte Website der eigentlichen Zielseite exakt nachgebildet ist. Gibt man dort seine Zugangsdaten ein, haben die Betrüger leichtes Spiel und können anschließend mit der Benutzererkennung zum Beispiel bei Internetauktionen mitbieten oder im Falle einer gefälschten Bank-Seite das Girokonto leer räumen.

Damit Pharming funktioniert muss zuerst ein Schadprogramm auf den Rechner des Nutzer gelangen. Dies geschieht über Viren, Trojaner oder Würmer, die sich zum Beispiel im Dateianhang von Spam-E-Mails verstecken. Pharming wird auch mittels "DNS-Cache-Poisoning" erreicht. Dabei wird

## INTERNET - Möglichkeiten und Dienste

der DNS-Cache des Providers durch bestimmte Methoden mit präparierten Einträgen "vergiftet", indem man ihm schon vor einer Anfrage eine gefälschte Antwort schickt. Diese gefälschte Antwort wird im Cache des DNS gespeichert und bei Anfragen von Clients zurückgeliefert. Somit erreicht den User die falsche IP-Adresse für eine Domain, die in Wirklichkeit auf den Server des Angreifers verweist. Da Cache-Poisoning-Angriffe seit langem bekannt sind, gibt es auch Methoden zur Abwehr. Kaum ein System lässt sich damit noch austricksen. Allerdings machen Fehlkonfigurationen und Schwachstellen auch heute noch Server und Caching-Proxies verwundbar.

Nach Angaben des Sicherheitsdienstleisters Messagelabs haben Betrüger einen neuen Phishing-Trick entwickelt, um an die Anmelde- und Konteninformationen von Bankkunden zu gelangen. Dazu versenden sie E-Mails mit Scripting Code, der die Hosts-Datei von Windows-Rechnern manipuliert. Die Betrüger tragen für bestimmte Banken eigene IP-Adressen in die Hosts-Datei ein, die zu präparierten Servern führen. Selbst wenn man keinem Link folgt und stattdessen die URL per Hand eingibt oder einen Bookmark aufruft, landet man durch diesen Trick der Angreifer auf der falschen Seite. Bislang habe man bei Messagelabs aber erst wenige solcher Mails abgefangen. Abhilfe soll des Abschalten von Windows Scripting Host bringen. Auch Viren und Würmer, etwa MyDoom, manipulieren die Hosts-Datei, um Antivirensoftware am Online-Update ihrer Signaturen zu hindern.

### Schutz vor Pharming

- Sie sollten immer eine aktuelle Virensoftware installiert haben.
- Sie sollten keine Dateianhänge von E-Mails unbekannter Herkunft zu öffnen.
- Niemals, also auch nicht von bekannten Absendern, sollte man ausführbare Dateien in Dateianhängen öffnen (exe, bat, pif oder com).
- Passwörter und Geheimnummern sollte man nur über sichere Internetverbindungen eingeben. Diese erkennt man zunächst daran, dass die Webadresse mit "https://" beginnt. Aber auch solche vermeintlich sichere Verbindungen können von Pharming-Betrügern auf präparierte Webseiten umgeleitet werden.
- Deshalb: Am unteren Rand der gängigen Browser befindet sich bei sicheren Verbindungen das Symbol eines Vorhängeschlosses. Per Mausclick auf dieses Symbol wird das Sicherheitszertifikat einer Webseite angezeigt. Meldet der Browser, dass er das Zertifikat eines Servers nicht verifizieren kann, ist Vorsicht geboten.

### Weiterführende Links

- [Goldene Regeln für schlechte E-Mails](#) Von Lars Kasper
- [Das Geheimnis der "blinden Durchschläge"](#) Von Matthias Opatz
- [E-Mail-Header lesen und verstehen](#) von Thomas Hochstein
- [Computervirus, Falschmeldungen und Legenden](#)
- <http://www.antisipam.de>
- <http://www.de.spam.abuse.net/>
- <http://www.iks-jena.de/mitarb/lutz/usenet/teergrube.html>
- [Computer Crime Research Center](#)
- [Heise Security](#)
- [Internet Storm Center \(ISC\)](#)
- [Security Focus](#)
- [Bundesamt für Sicherheit in der Informationstechnik](#)



[Zum Inhaltsverzeichnis](#)

---

Copyright © Prof. Jürgen Plate, Fachhochschule München

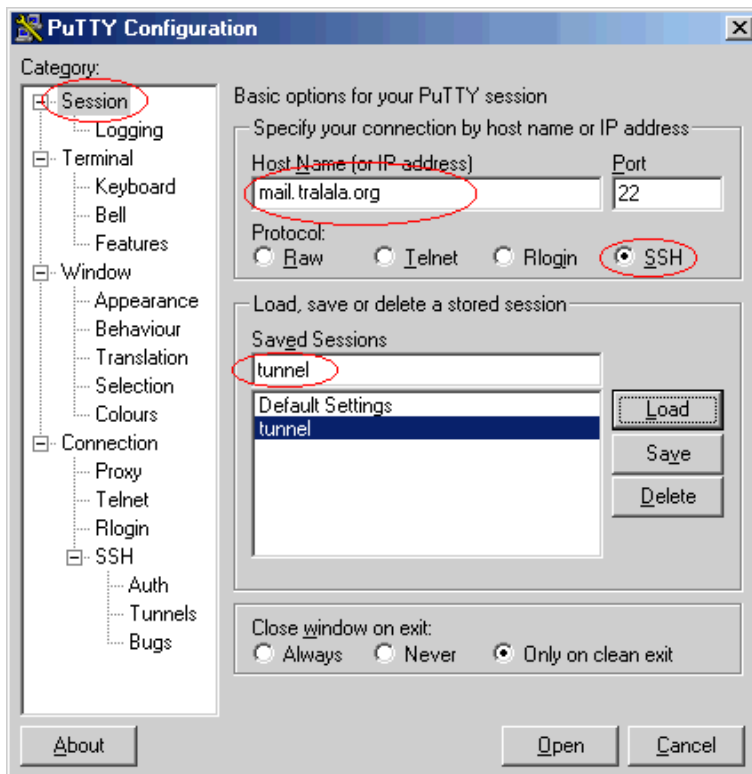


## SSH-Tunnel mit Putty

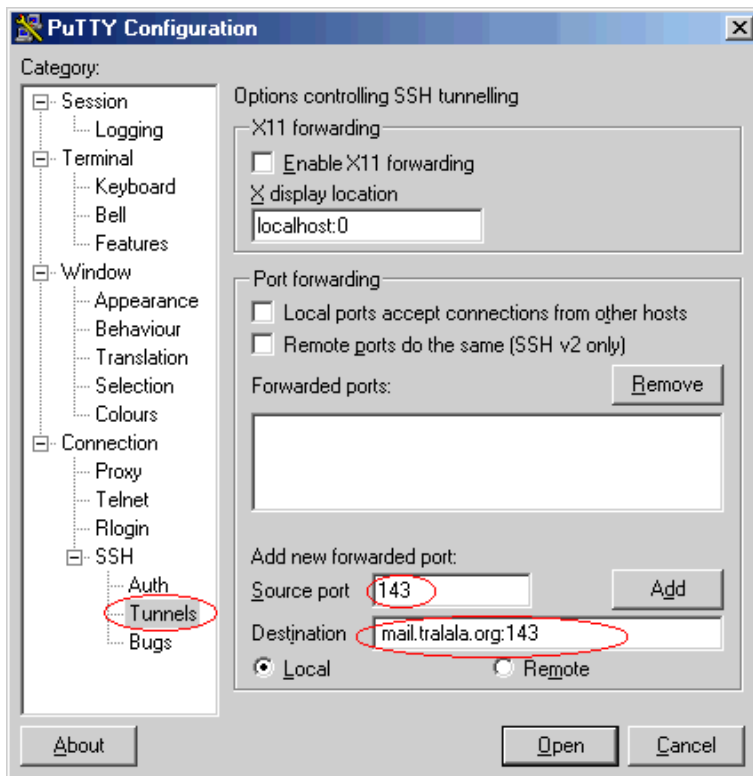
Die Situation ist vielleicht bekannt. Man sitzt mit seinem Laptop in irgendeiner Firma und ist ins dortige WLAN eingeklinkt. Jetzt möchte man schnell ein paar Mails lesen oder schreiben, hat aber keine Ahnung, welcher Rechner im Firmennetz für den Versand von Mail zuständig ist - und einfach einen fremden Mailserver in Anspruch nehmen ist ja auch nicht die feine Art. Also würde man gerne den heimischen Mailserver verwenden, doch der sagt "we do not relay" wenn man aus dem fremden Netz kommt. Da hilft dann nur noch ein SSH-Tunnel. Die Linux-User sind da fein raus, weil SSH zur Standard-Ausstattung zählt. Bei Windows geht es aber auch recht einfach, wie die folgende Anleitung zeigt.

Es wird der SSH-Client "Putty" verwendet, der als Freeware heruntergeladen werden kann. Putty ist als ausführbares Programm unter <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html> herunterzuladen. Eine Installation ist nicht nötig. Die Datei *Putty.exe* kann sofort ausgeführt werden. Wer will, kann sich ja noch ein Icon auf den Desktop legen.

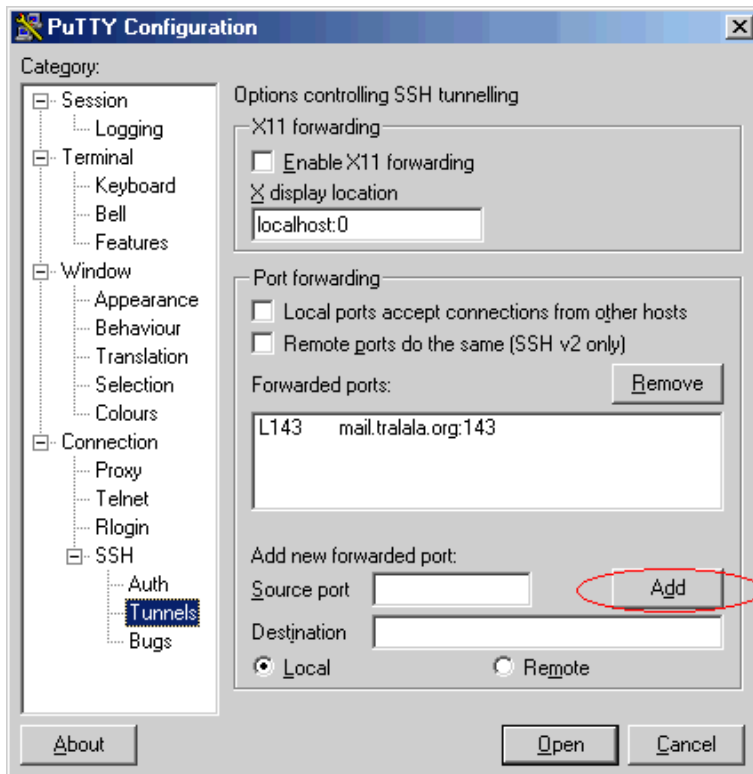
Das folgende Beispiel tunnelt die drei wichtigsten E-Mail-Protokolle. Sie starten Putty und erstellen eine neue Session. Dazu wird zuerst der Server eingegeben, zu dem der Tunnel aufgebaut werden soll. Als Protokoll wird SSH gewählt. Sie können auch gleich noch den Namen der Session (hier "tunnel") eingeben.



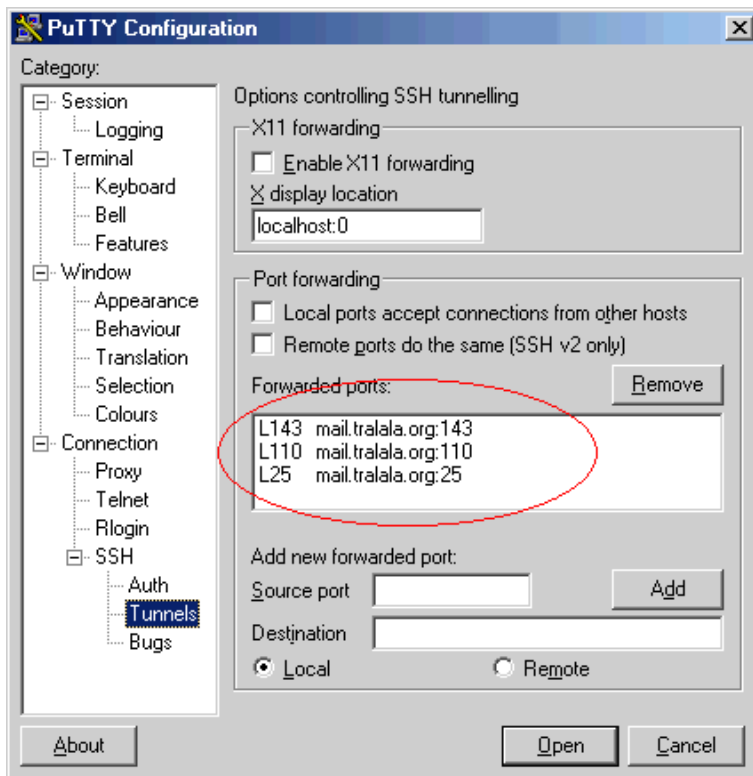
Danach geht es zum Menüpunkt "Tunnels" (zweiter von unten). Dort wird unter "Source Port" der Port eintragen, über den Sie lokal zugreifen wollen, im Bild ist das der IMAP-Port mit der Nummer 143. Dann unter "Destination" den Zielserver **mit** Port eingeben (*server.de:port*).



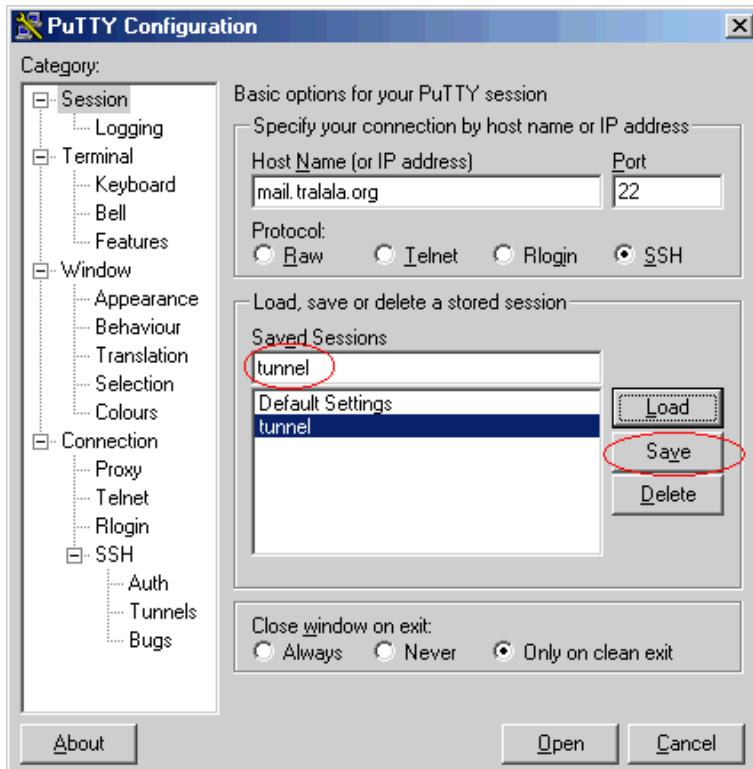
Mit Schaltfläche "Add" den Eintrag hinzufügen.



Genauso verfahren Sie mit weiteren Ports. Im Beispiel wurden noch POP3 (Port 110) und SMTP (Port 25) hinzugefügt - also alles, was man zum Abholen und Versenden von E-Mail braucht. Ihr Putty-Fenster sollte danach so aussehen:

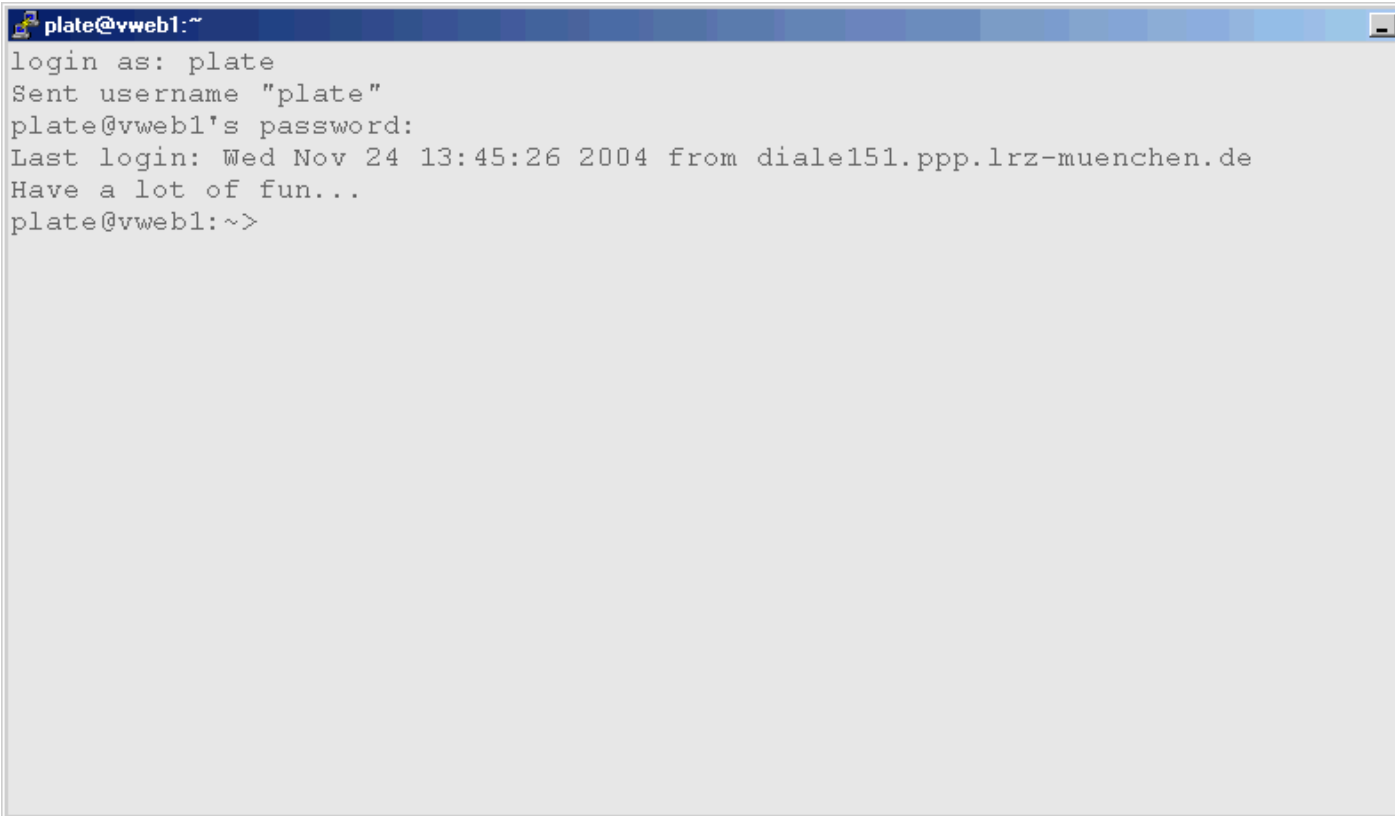


Nun geht es zu "Session" zurück. Falls Sie es nicht im ersten Schritt getan haben, geben Sie den Session-Namen (hier *tunnel*) ein und klicken Sie auf "Save".



Mit einem Klick auf den Session-Namen und anschließend auf "Load" läßt sich die Session jederzeit wieder laden.

Nun klicken Sie auf "Open" um die Verbindung zu öffnen. Es erscheint ein Login-Fenster, in dem Sie Usernamen und Passwort eingeben müssen.

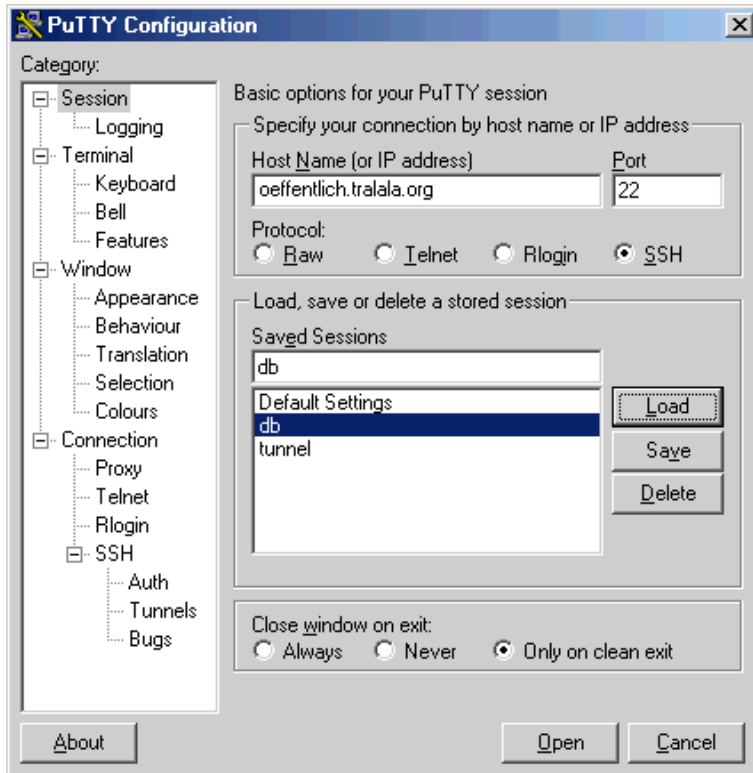
A screenshot of a terminal window with a blue title bar containing the text 'plate@vweb1:~'. The terminal output shows the following text:

```
login as: plate
Sent username "plate"
plate@vweb1's password:
Last login: Wed Nov 24 13:45:26 2004 from diale151.ppp.lrz-muenchen.de
Have a lot of fun...
plate@vweb1:~>
```

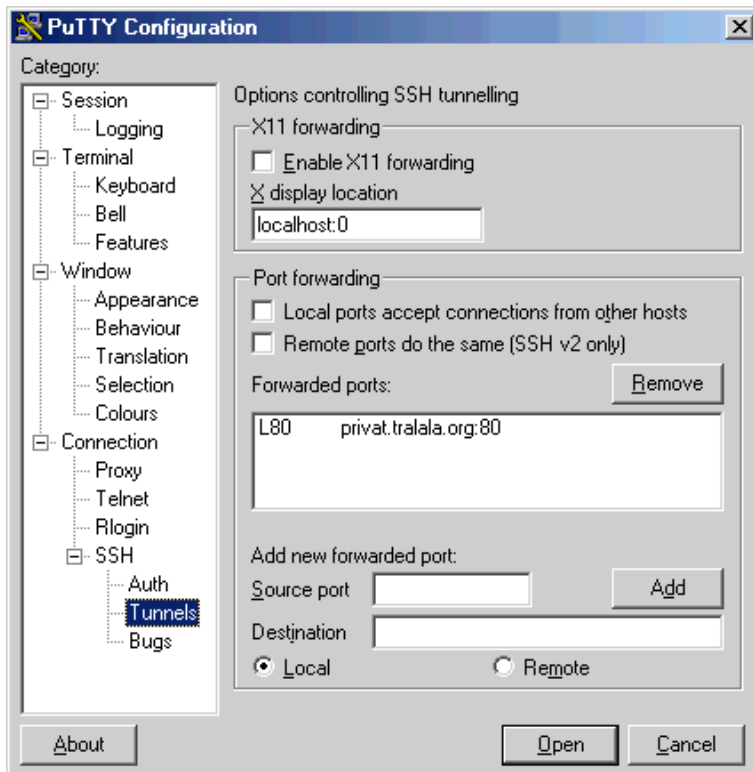
Bei erfolgreichem Login besteht der Tunnel, solange das Fenster offen ist. Zum Beenden der Verbindung geben Sie "exit" ein und drücken die ENTER-Taste. Alternativ können Sie STRG-D drücken.

Um nun Mail abzuholen oder zu versenden, müssen Sie bei Ihrem Mail-Client als Mailserver nicht mehr den ursprünglichen Server, sondern "localhost" angeben, da ja nun Ihr lokaler Rechner über den Tunnel verbunden ist.

Noch ein zweites Beispiel: Sie haben einen Rechner mit Web-Interface für eine Datenbank im internen Firmennetz stehen, der von außen nicht erreichbar ist (er heisst z.B. *privat.tralala.org*). Um ihn zu erreichen, bauen Sie einen Tunnel zu einem von aussen erreichbaren Rechner im Firmennetz auf (der heisse meinerwegen *oeffentlich.tralala.org*). Von ihm aus muss der "private" Rechner natürlich erreichbar sein. Dann sieht die Session folgendermassen aus. Als "Host" wird der öffentliche Rechner angegeben:



Beim Tunnel wird dann der private Rechner und der Port 80 eingetragen:



Nach dem Aufbau des Tunnels (mit Login wie oben) können Sie dann die Weboberfläche von *privat.tralala.org* durch die URL "<http://localhost/>" erreichen.

## INTERNET - Möglichkeiten und Dienste

*Copyright © FH München, FB 04, Prof. Jürgen Plate*

*Letzte Aktualisierung: 25. Nov 2004*

# - JAVA EINBLICK -

---

Ein Referat von Antje König

---

## Inhalt

- Das ist Java
- Das kann Java
- Die Geschichte von Java
- Hot Java / Netscape Navigator
- Die Programmiersprache
  - ◆ Die Eigenschaften
  - ◆ Ein Beispielprogramm
  - ◆ Kompilierung
- HTML-Implementierung
  - ◆ Ein Beispiel
  - ◆ Attribute
  - ◆ Parameter
  - ◆ Noch ein Beispiel
- JDK - Java Development Kit
- Kommerzialisierung?
- JavaScript
- Quellen / Literatur
- Die wichtigsten Links

---

## Das ist Java

Java wurde von der Firma **Sun Microsystems** (Workstations, Unix) entwickelt. Java ist eine plattformunabhängige, objektorientierte Programmiersprache, die es ermöglicht, WorldWideWeb-Seiten interaktiv zu gestalten.

Mit Java programmierte Applikationen (Applets), die per HTML in Web-Seiten integriert werden, werden beim Öffnen der Seite übers Internet automatisch gestartet.

Damit ist es möglich, die bislang statische Informationsabfrage im Web durch die interaktiven Möglichkeiten dieser online ausführbaren Programme zu ergänzen.



## Das kann Java

Theoretisch sind den Anwendungsmöglichkeiten keine Grenzen gesetzt. Da die Sprache noch relativ jung ist, experimentieren interessierte Programmierer zunächst mit einfachen Dingen, die als "normale", "nicht-online" Software nichts Neues wäre.

Zur Zeit finden sich verschiedene Kategorien von integrierten Applets im WWW. Hauptsächlich stößt man auf Animationen, wie Laufschriften, hüpfende Icons und bewegte Grafiken. Aber auch Spiele, Musik, Client/Server-Zugang, Finanzplanungs-Programme oder Börsenapplikationen kann man beim "surfen" finden. Und es wird ständig mehr.



---

## Die Geschichte von Java

Ursprünglich wurde die Programmiersprache für die Gerätesteuerung entwickelt. Das Entwickler-Team bei Sun fand, daß die existierenden Sprachen C und C++ für Steuerungssoftware ungeeignet sind, da sie für bestimmte Chips kompiliert werden und bestimmte Bibliotheken benutzen. Für Geräte mit meist langer Lebensdauer, wie Toaster, Videorecorder, Telefone u.ä., mußte über eine neue Sprache nachgedacht werden. Die Sun-Leute waren überzeugt, daß die Zukunft in kleinen Programmen für diese Consumer devices liegen würde. 1990 entwickelte **James Gosling** eine neue objektorientierte Programmiersprache namens **Oak**, mit der dann das "Green" Projekt mit dem Kleinst-Computer \*7 (Star seven) begonnen wurde.

Dabei entstand auch das **Zeichentrick-Maskottchen Duke**, das die Anwender durch den virtuellen Haushalt navigierte.

Auch wurde an eine Verwendung für die SetTop Boxen des Interaktiven Fernsehens gedacht, doch 1994 kam das Aus, da niemand Oak lizensieren wollte. Zu diesem Zeitpunkt jedoch entdeckte die breite Masse das Internet. Das Sun-Team fand, daß diese neue plattformunabhängige Sprache hervorragend zur Programmierung von Web-Anwendungen geeignet wäre und stellte sie unter dem Namen **Java** im Frühjahr 1995 der Internet-Gemeinde vor. Ein Jahr später scheint sich die Prophezeiung der Java-Entwickler zu bewahrheiten, daß Java das Internet revolutionieren wird. Wie ein Mitarbeiter von Sun treffend formulierte: "Java ist eine Lösung, die nur noch auf das passende Problem gewartet hat."

Übrigens, die häufige Darstellung von Kaffeetassen im Zusammenhang mit der Sprache erklärt sich dadurch, daß Java in den USA umgangssprachlich "Kaffee" bedeutet, der auch das Hauptexportprodukt der gleichnamigen Insel darstellt.



---

## Hot Java / Netscape Navigator

Die Anwendung der Java-Applets im WWW wird erst durch einen **Browser** ermöglicht, der die Tags (Anweisungen) und Parameter der HTML-Implementierung versteht. **Hot Java** von Sun war der erste

Browser, der dies ermöglichte. Hot Java, der komplett in Java geschrieben ist, kann also nicht nur HTML interpretieren, sondern auch Java-Applets laden und ausführen. Er ist z.Zt. für Sun Solaris 2.3, 2.4, 2.5, für Windows NT, Windows 95 sowie für Apple Macintosh verfügbar. Auch Netscape hat seinen Navigator 2.0 Java-kompatibel gemacht. Das heißt konkret, daß die Java Virtual Machine, der Bytecode-Interpreter, in den Browser eingefügt wurde.



---

## Die Programmiersprache

Java ist sehr stark an C++ angelehnt, hat aber Besonderheiten, die es für die geplante Anwendung im Netz besonders auszeichnen sollen. Am leichtesten werden es ProgrammiererInnen haben, denen die Syntax von C++ geläufig ist. Für alle NichtprogrammiererInnen ist Java genauso leicht oder schwer zu erlernen wie jede andere Sprache, auch wenn Sun behauptet, Java sei besonders einfach.

### Die Eigenschaften

#### - Objektorientiert

In Java geschriebene Programme benutzen Objekte. **Objekte** werden in zwei Bestandteile unterteilt, Datenelemente und die dazugehörigen Funktionen (Methoden). Inhalte von Datenelementen repräsentieren den Zustand, in dem ein Objekt sich gerade befindet. Funktionen sind Operationen, die ein Datenobjekt von einem Zustand in einen anderen versetzen. Die Gesamtheit von Objekten mit gleichen Eigenschaften wird als Klasse bezeichnet. Objektorientiertes Programmieren ist die Zusammenstellung von Klassenbeschreibungen, d.h. die Beschreibung der Datenelemente, die jedes Objekt der Klasse enthält, sowie der Funktionen, die auf jedes Objekt der Klasse anwendbar sind. Diese sind z.B. im Rahmen eines größeren Programmpaketes wiederverwendbar. Somit kann man sich im Laufe der Zeit eine umfangreiche Bibliothek (**Klassenbibliothek**) verschiedener Objekte anlegen. Ein Satz Bibliotheken für Standardaufgaben (wie z.B. Ein/Ausgabe oder Graphik) wird zur Sprache mitgeliefert.

#### - Plattformunabhängigkeit

Die Plattformunabhängigkeit/Architekturneutralität ergibt sich aus der Tatsache, daß Java-Programme zunächst in neutralen Byte-Code kompiliert werden. **Byte-Codes** ähneln Maschinenbefehlen, sind jedoch nicht für eine bestimmte Maschine spezifisch. Die Quellcodes in Java werden zu Dateien vom Typ **.class** kompiliert, die das Programm in Bytecode enthalten. Die Bytecodes können nun auf jeder Plattform laufen, die Java unterstützt. Sie werden quasi beim Starten interpretiert und ausgeführt.

#### - Multithreading

Threads sind parallele Aktionen, die ein Programm gleichzeitig ausführen kann. Das heißt, ein **Thread** kann eine Berechnung durchführen, wobei gleichzeitig ein anderes Thread eine Benutzerinteraktion ermöglicht. Es gibt also weniger Wartezeiten. Java hat leicht benutzbare Synchronisationseigenschaften, die die Schwierigkeiten der Programmierung solcher Umgebungen einfacher machen sollen.

#### - Sicher und robust

Java-Programme können vor der Ausführung verifiziert werden, da sie keine Zeiger haben und in Bytecode vorliegen. Die Verifizierung wird von Web-Browsern benutzt, um sicherzustellen, daß keine Viren enthalten sind. Java verwendet nicht Adressen aus Zahlen, sondern Namen für Funktionen und Methoden, die leicht überprüft werden können. So kann kein Java-Applet etwas ausführen oder auf etwas zugreifen, was nicht ausdrücklich im Verifizierungsprozess definiert worden ist. Dadurch, daß

jeder Speicherzugriff geprüft wird, kommt es nicht zu Computerabstürzen.

### - Garbage Collector

Wird ein Speicherbereich des Rechners nicht mehr benötigt, muß ein Programmierer, der in C oder C++ (und vielen anderen Sprachen) programmiert, darauf achten, daß das Programm ihn zur Neubenutzung wieder freigibt. Diese Speicherverwaltung erfordert große Genauigkeit. Bei Java erledigt dies ein eingebautes Programm, der Garbage Collector, das den Speicher scannt und nicht mehr gebrauchte Speicherbereiche wieder freigibt.



---

## Ein Beispielprogramm

Auf die Syntax von Java kann hier nicht näher eingegangen werden. Ausführliche Erläuterungen dazu findet man unter <http://www.javasoft.com/hooded/language-ref.html>.

Als exemplarisches Beispiel hier nur das obligatorische "Hello world" Programm.

```
1: /*2: *Datei: Helloworld.java3: */4: public class Helloworld5: {6:     public static void main (
```

### Erklärung:

**Zeile 1-3:** Kommentar

**Zeile 4:** Deklaration der Klasse, der Compiler übernimmt den Namen "HelloWorld" (und nennt das Programm helloworld.class)

**Zeile 6:** Aufruf der Methode / Funktion,

- **main** heißt: diese Klasse hat eine Methode, und die "oberste" Methode heißt wie bei "C" main ()
- **public** heißt: die Methode kann von überall aufgerufen werden
- **static** heißt: alle Instanzen der Klasse sind inbegriffen
- **void** heißt: das die Methode keinen Wert zurückgibt
- Das Argument ist eine Zeichenkette (**String**) namens args

**Zeile 8:** Die Bildschirmausgabe "HelloWorld" erfolgt durch den Befehl **println**, der zu der Klasse **out** gehört, die Teil des **System**-Objekts ist. Der Befehl beinhaltet eine Zeilenschaltung.

### Kompilierung:

Der Quellcode heißt hier Helloworld.java. Wird er mit dem Java-Compiler bzw. mit dem Befehl `javac` kompiliert, wird eine Datei mit dem Namen Helloworld.class erzeugt, die jetzt auf allen Plattformen mit Java-Interpreter die Bildschirmausgabe "Hello world!" erscheinen läßt.





## HTML Implementierung

Alle HTML-Befehle stehen in sogenannten Tags, die durch diese <> spitzen Klammern definiert werden. Fast alle HTML-Anweisungen haben ein einleitendes und ein abschließendes Tag.

Dazwischen ist die Gültigkeit der Anweisung angegeben.

So wird auch für die Einbindung der Java Applets ein bestimmtes Tag benötigt, welches die Browser, die Java-kompatibel sind (Netscape, HotJava), interpretieren können. Andere Browser ignorieren das unbekannte Tag und zeigen das Applet nicht an.

Dieses <applet> Tag schließt den Namen, die Breite und Höhe sowie die Parameter ein.

### Als Beispiel:

1: <applet code="HelloWorld.class" width=100 height=30>

2: <param name=text value="Hallo, Welt!">

3: Sie benötigen einen Java-kompatiblen Browser!

4: ;/applet>

### Erläuterung:

**Zeile 1:** Der Name des Applets sowie Breite und Höhe: die notwendigen Standardattribute (code, width, height)

**Zeile 2:** Die Applet-Parameter sind Attribute außerhalb des Standards, nur für dieses Applet gültig. Hier enthält Parameter "text" eine Zeichenkette

**Zeile 3:** Alternativer HTML-Inhalt, der angezeigt wird, wenn der Browser Java nicht versteht

**Zeile 4:** Ende des Applets

## Attribute

Also, es gibt die Attribute, die in dem Start-Tag <applet> spezifiziert werden. Hier unterscheidet man **die notwendigen** (code, width, height) **und die optionalen Attribute**.

Optionale Attribute sind z.B.:

- codebase ( Basis URL des Applets, ist nicht am gleichen Ort wie die HTML-Seite),
- alt (alternativer Text, der von reinen Text-Browsern angezeigt wird),
- align (bestimmt die genaue Position des Applets auf der Seite, es stehen die Ausrichtungen left, right, top, texttop, middle, baseline, bottom zur Verfügung).
- vspace, hspace ( der vertikale bzw. horizontale Abstand um das Applet herum. Wird nur benutzt, wenn das align-Attribut auf left oder right steht.)

## Parameter

Daneben werden oft Applet-spezifische **Parameter** angegeben. Sie werden in dem gesonderten <param>-Tag definiert. Das <param>-Tag hat zwei Attribute, name und value, so daß ein Name und der dazugehörige Wert spezifiziert werden kann.

Häufige Verwendung finden Parameter bei Animationen. Sie machen z.B. Angaben über: area, background, border, c\_color, edges, font, highlight, images, maxwidth, model, orientation, positions, repeat, scale, sounds, speed, startup, text, u.s.w.

**Bsp:**

```
<applet code =ImageLoopItem width=80 height=90 align=right>  
<param name=nimgs value=10>  
<param name=img value=duke>  
<param name=pause value=1000>  
</applet>
```

Hier wird eine Imagesequenz wiederholt abgespielt, um eine Animation zu erzeugen.

Der Parameter **img** spezifiziert den URL (Uniform Ressource Locator), von dem die Bilder geladen werden.

Die Zahl der Bilder in der Animation wird durch den Parameter **nimgs** festgelegt.

Durch **pause** wird eine Pause in Millisekunden angegeben, die zwischen jeder Wiederholung der Sequenz liegt.



---

## JDK - Java Development Kit

Das **Entwicklerwerkzeug** "Java Development Kit" von Sun ist ein Paket mit den wichtigsten Dingen um in Java zu programmieren. Das JDK kann man direkt über das Netz von Sun (<http://java.sun.com/>) downloaden. Die andere Möglichkeit wäre, die Java-CD Edition 1 bei Sun Deutschland kostenlos anzufordern.

Die **Bestandteile des JDK** sind:

- der Java-Compiler *javac*
- der Java-Interpreter *java*
- der (nur zeichenorientierte) *Debugger jdb*
- der *Applet Viewer* als interaktives Testwerkzeug
- die umfangreiche API Documentation sowie *API User's Guide.html*
- die Standard-Bibliotheken *Java shlb*

In dem Paket sind auch diverse Applets mit vollem Quelltext enthalten.

Das JDK unterstützt zur Zeit die **Plattformen** Solaris (SPARC), Windows NT, Windows 95 und Apple Macintosh. Fremdfirmen kündigten bereits vollständige Entwicklungsumgebungen an. Borland plant etwas unter dem Codenamen Latte. Symantec hat eine C++ Compilererweiterung mit Namen Espresso veröffentlicht.



## Kommerzialisierung?

Mit dem jeweiligen Browser oder der passenden Helper-Application ist es für jeden NutzerIn möglich, die **Source-Codes** der aktuellen HTML-Site anzusehen. Das hat einen gewissen Charme, da es so möglich ist, von anderen zu lernen. Zusätzlich ist es ebenso kein Problem, die in den Seiten eingebauten Originalbilder per Mausklick auf den eigenen Rechner zu kopieren.

Da von in Java geschriebenen Programmen nur der Bytecode aufs Netz gestellt wird, ist es hier nicht möglich, sich den Quellcode anzusehen. Das hat gewiß den Vorteil, daß die ProgrammiererInnen die Kontrolle über ihr **geistiges Eigentum** auch in kommerzieller Hinsicht behalten.

Doch dazu ein **Kommentar** aus der Zeitschrift Gateway:

### "Eingriff in die Internet-Kultur

Bei der Verwendung im Internet ergeben sich jedoch einige negative Nebeneffekte: Durch Java wird es nicht mehr notwendig sein, den Source-Code der Applikationen zur Verfügung zu stellen, da die kompilierte Klasse voll ausreicht. Schon heute bietet kaum eine der kommerziellen Web-Sites, die Java-Spielereien in ihrer Homepage haben, den Zugriff auf den Source an. Auch viele Freizeitprogrammierer, werden der alten Tradition der "Free Software" den Rücken zuwenden und ihre Utilities nur binär zum Gebrauch zur Verfügung stellen. Sollte dann auch noch electronic Cash eingeführt sein, wird es eine neue Form von Shareware geben: der Code kann nur gegen Geld per WWW geladen und ausgeführt werden. Hierzu plant Netscape übrigens, bei der Übertragung von Objektklassen ihr Secure-Socket-Layer-Protokoll (SSL) einzusetzen, welches vor unzulässigen Modifikationen des Codes schützen soll. Das könnte dazu beitragen, Java zu einem Medium für Netzwerkkommerz zu machen."



---

## JavaScript

JavaScript ist eine **Macrosprache**, eine einfach zu verstehende **Scriptsprache** von Netscape Navigator. Andere Browser unterstützen JavaScript zur Zeit nicht. Java Applets werden als vorkompilierte Programme vom Netz geladen und vom jeweiligen Browser bzw. Java-Interpreter ausgeführt.

JavaScript dagegen ist im **Klartext** in der www-Seite eingebunden. Dadurch ist es möglich, ohne eine Netzwerkübertragung auf Interaktionen zu reagieren. Diese Scriptsprache ist auf keinen Fall mit der komplexen Programmiersprache Java von Sun zu verwechseln. Für das Script-Schreiben sind keine umfangreichen Programmierkenntnisse erforderlich, dafür werden jedoch auch nicht alle Elemente von Java unterstützt.

JavaScripts können auf viel mehr Daten auf dem lokalen Rechner zugreifen als normale Java-Applets. Es kann dadurch Sicherheitsprobleme geben. Netscape soll diese Probleme jedoch mit der neuesten Navigator-Version behoben haben. Weitere Informationen direkt von Netscape auf dessen JavaScript-Seite:

[http://www.netscape.com/comprod/products/navigator/version\\_2.0/script/index.html](http://www.netscape.com/comprod/products/navigator/version_2.0/script/index.html)

## Syntax:

Mit dem `<script language="LiveScript">`-Tag wird das Script direkt in der HTML-Seite begonnen, und mit `</script>` beendet. Die JavaScript-Befehle sind durchaus sofort verständlich, wenn man denn der englischen Sprache mächtig ist. Neu programmierte Funktionen werden bereits im Head der Seite definiert, um dann von den NutzerInnen im Body an geeigneter Stelle im JavaScript aktiviert zu werden. Ein guter Einführungslehrgang ist hier zu finden:

[INTRODUCTION TO JAVASCRIPT](http://rummelplatz.uni-mannheim.de/~skoch/js/script.htm) von Stefan Koch:  
<http://rummelplatz.uni-mannheim.de/~skoch/js/script.htm>  
<http://www.webconn.com/java/javascript/intro>

Und die Übersetzung ins Deutsche von Veikko Wuensche:  
<http://www.hansenet.de/vw/PW/>

## Auch hier ein Beispiel:

```
<script language="LiveScript">
<!-- Hiding
today = new Date()
document.write("Die aktuelle Uhrzeit ist: ",today.getHours(),":",today.getMinutes())
document.write(".....")
document.write("Das heutige Datum ist: ",today.getDate()," ", today.getMonth()+1,"
",today.getYear());
// end hiding contents -->
</script>
```

### Hier ist das Script realisiert!

Hier wird also mit Standard-Funktionen , z.B. **today.getDate()**, auf die rechnerinternen Einstellungen von Datum und Uhrzeit zugegriffen und mit **document.write** auf dem Bildschirm angezeigt. Und um sicher zu stellen, daß alte WWW-Clients den Code nicht versuchen als HTML-Text darzustellen, ist er als Kommentar (**<!-- Hiding**) eingerahmt.



---

## Quellenangaben / Literatur:

- "Java Applets erstellen und nutzen" - van Hoff, Shaio, Starbuck; Addison-Wesley 96
- "Java im Detail" - Infobroschüre von Sun, März1996
- "Java, Koffein fürs Internet" - Veranstaltung 3.April 96, Stadthalle Sindelfingen
- "Java. Bahnt sich die nächste Internet-Revolution an?" - Gateway September 95
- " Was ist Java?", "Java soll den Umgang mit den Anwendungen revolutionieren" - COMPUTERWOCHE Nr. 48 vom 1. Dezember 1995
- "Heißer Kaffee - Programmieren mit Java" - c't, Februar 96

## INTERNET - Möglichkeiten und Dienste

- "Bewegung auf dem Netz" - Zeitschrift UNIXopen, AWi Verlag
- "Kaffe-Auslese" - c't April 96
- "Applets, schöne Applets" - Artikel, Verlag H.Heise, April 96
- "Verletzungsgefahr" - c't, Mai 96

---

### Die wichtigsten LINKS:

- <http://java.sun.com> - Die offiziellen Javaseiten von Sun
- <http://java.sun.com/starter.html> - Getting started
- <http://java.sun.com/doc/programmer.html> - Info für Java Programmierer
- <http://www.javasoft.com> - Die eigens gegründete Tochterfirma JavaSoft
- <http://www.gamelan.com/> - Gamelan - Übersicht von Applets
- <http://www.digitalfocus.com/> - "How Do I"? - Antworten auf häufig gestellte Fragen
- <http://www.sun.de> - Deutsche Sun Seiten mit Infos zu Java
- <http://java.pages.de> - Eine Sammlung deutscher Java Ressourcen
- <http://acc.de/java/wasisjava.html> - Deutsche Java Sammlung von Christoph Bergmann

Weitere interessante URLs sind bereits auf den angegebenen Seiten gut zusammengestellt.



---

Antje König, 08. Mai 1996

[Homepage](#)

[Mail / Post](#)