Vorlesung Informationstechnik

Modul 4 - Informationsverbreitung

Inhaltsverzeichnis

1 Einleitung

Die Informationsverbreitung erfolgt heute im Wesentlichen über Kommunikationsnetze. In diesem Abschnitt sollen daher Grundlagen der Kommunikation zwischen Mensch und Maschine im Vordergrund stehen. Wie eine lokale oder globale Verbreitung dieser Informationen erreicht wird, welche Schnittstellen zwischen den Kommunikationsteilnehmern zur Verfügung stehen oder auch Probleme bei einer Vernetzung, soll hier Gegenstand sein.

Daher wird zunächst die Kommunikation als Begrifflichkeit geklärt und verschiedene Wege der Kommunikation aufgezeigt werden. Weiter wird auf verschieden Netzwerke und die Topologie sowie Funktionsweise dieser Netzwerke eingegangen. Als größtes Netzwerk wird das Internet in seinem Aufbau und Funktion erläutert, sowie Probleme und Chancen dieses Mediums angerissen. Als Sicherheitsrisiko innerhalb dieses Mediums werden z.B. Viren und andere Probleme vorgestellt und im Folgenden Gegenmaßnahmen aufgezeigt. Wichtig für die Informationsverbreitung und besonders der Informationserhaltung ist die Datensicherheit. Hierzu werden mögliche Lösungsansätze und Strategien erläutert.

2 Grundlagen der Kommunikation

2.1 Was ist Kommunikation?

Für den Menschen spielt seit jeher die Kommunikation eine bedeutende Rolle. Das Mitteilen oder Verständigen, was unter Kommunikation zu verstehen ist, kann dabei in verschiedenen Formen stattfinden. Ob anhand von Sprache, Gesten, Bildern, Zeichen, Geruch, etc. bleibt das Ziel einer jeden Kommunikation Informationen zu senden oder zu empfangen. Es werden Daten z.B. in Form von Wörtern weitergegeben, die eine Information transportieren und einem Zielobjekt übergeben. Je nachdem wie der Empfänger diese Daten interpretiert, entwickelt sich daraus Wissen. Das muss aber nicht so sein, hierfür ist der Schulunterricht ein gutes Beispiel, wo nicht immer jedes gesprochene oder geschriebene Wort gleich in Wissen umgesetzt wird. Eine Kommunikation findet dennoch statt.

Der Begriff "Kommunikation" bezeichnet **jede Art von Verständigung und Informationsaustausch** zwischen:

- **Lebewesen und Lebewesen** (Sprache, Gestik, Verhalten etc.)
- **Lebewesen und Maschine** (von Menschen oder Maschinen hergestellten Gebilden, zum Beispiel Programmieren von Videorekordern, Fahrkartenautomat bedienen, PC-Programm installieren)
- **Maschine und Maschine** (z. B. Daten werden vom Rechner an den Drucker übermittelt)

2.2 Arten der Kommunikation

2.2.1 Kommunikation zwischen Mensch und Mensch

Es gibt eine Reihe von Wissenschaftlern die sich mit der Kommunikation zwischen Menschen beschäftigen. Definitionen lassen sich viele finden. Eine der verbreitetsten Theorien ist das Kommunikationsmodell von **Shannon & Weaver** (Abbildung 2-1). Es entstand 1949 als rein technisch orientiertes Modell. Das ursprüngliche Ziel war es, ein Modell für eine optimale Kommunikation an die amerikanische Armee zu liefern. Es besagt, dass die Kommunikation ein linearer Prozess ist, in dessen Mittelpunkt das Signal steht. Das Prinzip des Shannon & Weaver-Modells ist, dass

jede menschliche Kommunikation eine Quelle (information source) hat. Diese Quelle ist der Sender, der seine Nachricht (message) in Form eines Kodes über einen Kanal (transmitter) weitergibt. Es können dabei Störungen (noise source) auftreten, wie zum Beispiel das Rauschen beim Telefonieren.

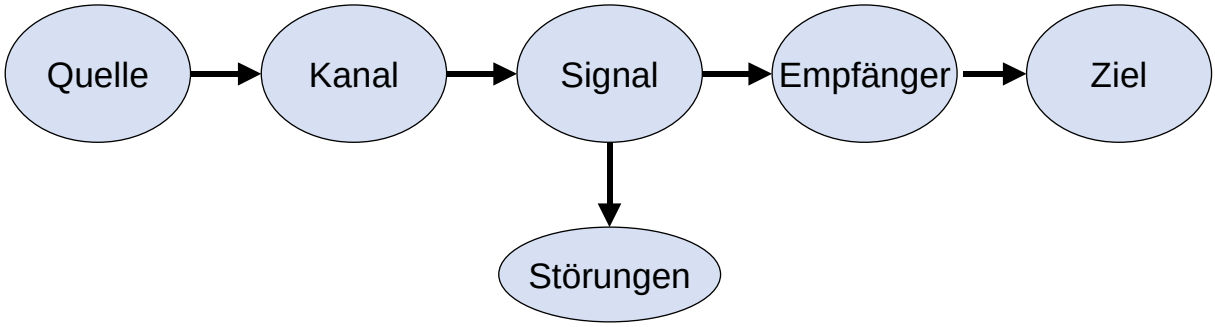

Abbildung 2-1: Kommunikationsmodell von Shannon & Weaver

2.2.2 Kommunikation zwischen Mensch und Maschine

Die Kommunikation zwischen Lebewesen und Maschine, also **Mensch und Maschine** lässt sich wie folgt charakterisieren:

- Es muss ein **Austausch** von Informationen stattfinden. (Das Bedienen einer Ständerbohrmaschine ist also noch kein Mensch-Maschine System. Die Programmierung einer CNC-Drehmaschine jedoch erfolgt durch diesen Informationsaustausch)
- Der Informationsaustausch ist **wechselseitig.** Ein Informationsfluss in eine Richtung ist nicht ausreichend. Es basiert auf dem Prinzip:
- **Eingabe** (durch den Menschen) – **Verarbeitung** (durch die Maschine/Computer) – **Ausgabe** (durch die Maschine)
- In einem Mensch-Maschine-System verfolgt der Mensch bestimmte **Ziele**, wie etwa den sicheren und effektiven Ablauf eines Prozesses. Das kann die Erzeugung von elektrischer Energie aus fossilen Brennstoffen oder die Beförderung von Passagieren in einem Flugzeug sein.

2.2.3 Kommunikation zwischen Maschine und Maschine

Bei der Kommunikation zwischen Maschine und Maschine werden Informationen ohne die Beteiligung des Menschen ausgetauscht. Die Informationsverbreitung wird

zwar durch den Menschen veranlasst, der Austausch der Informationen wird jedoch der Maschine überlassen. Beispiel hierfür sind computergestützte Netzwerkverbunde wo Daten von einem Benutzer in einen Computer eingegeben werden und mittels verschiedener Protokolle zu dem jeweiligen Zielrechner gelangen. Bei der letzteren Kommunikation, ist der genaue technische Ablauf dem Benutzer i.d.R. nicht bekannt. Die vernetzten Rechner kommunizieren untereinander und geben die Daten anschließend an einen Benutzer weiter. Dieser Ablauf soll in den folgenden Kapiteln näher erläutert werden.

2.2.4 Telekommunikation

Werden die im vorherigen Kapitel behandelten Informationen zwischen den Beteiligten in Form von Sprache, Text, Bildern oder Daten übermittelt, so wird von Telekommunikation gesprochen. Die Telekommunikation kennzeichnet alle Übertragungswege vom Telefon bis zum Nachrichtensatelliten.

Sie beinhaltet jede Übertragung, Sendung oder den Empfang von Zeichen, Signalen, Schriftbildern oder Tönen und Nachrichten, gleich welcher Art, mittels Leitungen, Radio oder optischen sowie anderen, elektromagnetischen Systemen. Um Telekommunikation durchführen zu können, müssen Übertragungswege vorhanden sein und Verbindungen zwischen den Teilnehmern hergestellt werden. Dies erfolgt durch Telekommunikationsnetze. Je nach Vermittlungsprinzip wird bei den Weitverkehrsnetzen zwischen Netzen mit Leitungsvermittlung und Datenpaketvermittlung, sowie zwischen herkömmlichen Netzen und solchen für Mobilfunk unterschieden. Neben den Netzen ist die Telekommunikation geprägt durch die Telekommunikationsdienste. Unter einem Telekommunikationsdienst ist ein bestimmtes Angebot eines Anbieters zur Durchführung der Kommunikation zu verstehen. Es wird unterschieden zwischen den reinen Übertragungs- und Vermittlungsdiensten, den so genannten Transportdiensten oder Übermittlungsdiensten, den Telediensten, bei denen die Endgeräte berücksichtigt werden und den Mehrwertdiensten. Im Konsumentenumfeld gibt es als neue Dienste die so genannten Verteildienste und die interaktiven Dienste. Zu der erstgenannten Gruppe gehören u.a. Pay-per-View, Pay-per-Channel, zu der zweiten Gruppe u.a. Video-on-Demand, Videospiele, Teleshopping.

2.3 Kommunikationsnetze

Einfache Kommunikationsmodelle könnten folgende Struktur haben: Teilnehmer 1 will eine Nachricht übermitteln. Diese Nachricht wird durch einen Wandler in ein

Signal umgewandelt. Nachdem Senden des Signals wandelt erneut ein Wandler das Signal in eine Nachricht zurück. Teilnehmer 2 kann als Empfänger diese Nachricht empfangen. (Abbildung 2-2). Hier wird das Mensch-Maschine und Maschine-Mensch-System durch den Nachrichtenfluss deutlich. Wie der genaue technische Ablauf einer solchen Informationsverbreitung funktioniert, soll im folgendem Kapitel anhand von computergestützten Netzwerken verdeutlicht werden.

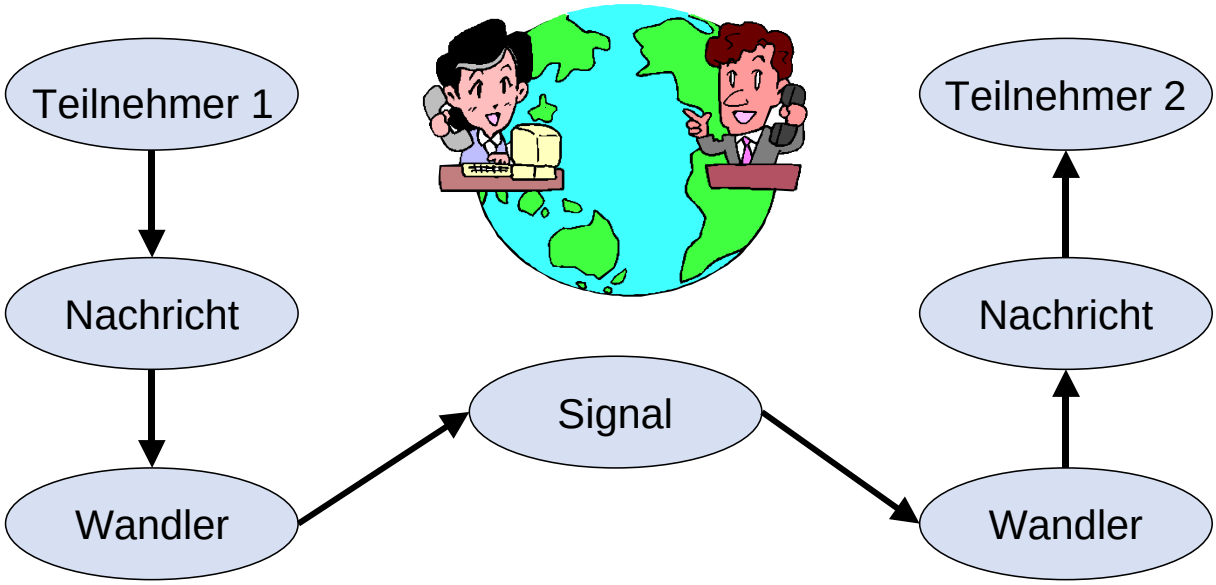

Abbildung 2-2: Einfaches Kommunikationsmodell

3 Netzwerk

Der Austausch von Informationen während einer Kommunikation erfolgt über Daten. Diese Informationen können in verschiedensten Formen vorhanden sein. Um die Kommunikation zu standardisieren, werden die Informationen mittels eines Computers in digitale Daten umgewandelt. Die Rückwandlung der Informationen erfolgt wiederum durch Computer. Zum Transport der Daten werden die Computer miteinander verbunden. Diese Verbindungsstrukturen werden aufgrund ihres Aufbaus Netzwerke genannt.

In diesem Abschnitt sollen die verschiedenen Netzwerkstrukturen mit ihren Funktionsweisen erläutert werden, um einen groben Überblick über das Thema zu erhalten.

3.1 Definition Netzwerk

Ein Netzwerk ist eine Verbindungsstruktur aus zwei oder mehr Computerstationen, die direkt (mit Kabel) oder indirekt (z.B. Funk) zum Zweck der Datenkommunikation miteinander verbunden sind. Die größtmögliche, nämlich weltweite Variante eines Computer-Netzwerks begegnet uns unter dem Stichwort „Internet“.

3.2 Gründe und Ziele einer Vernetzung

Ein Computernetzwerk bietet einige Vorteile gegenüber Einzelplatzlösungen.

- Kommunikation
- Steigerung der Effektivität im Datenverbund
- Kostensenkung im Funktionsverbund
- Datensicherung
- Absicherung der Verfügbarkeit
- Optimierung der Rechnerauslastung
- Optimierung der Wartung

Kommunikation

Netzwerke dienen dem Informationsaustausch, der **Kommunikation**. Daten und Nachrichten können innerhalb eines Netzwerkes von Benutzern (User) abgerufen und versandt werden. Eine Anbindung an das Internet ermöglicht einen weltweiten Austausch von Informationen.

Steigerung der Effektivität im Datenverbund

Daten können zentral abgelegt werden, sodass berechtigte Benutzer sie von jeder dem Netzwerk angebundenen Station abrufen können. Allgemein wird hier von einem so genannten **Datenverbund** gesprochen.

Kostensenkung im Funktionsverbund

Hochwertige Geräte müssen nicht für jede Computerstation angeschafft werden, sondern können innerhalb eines Netzwerkes von jeder Station genutzt werden. Es kann hier von einem **Funktionsverbund** gesprochen werden. Dies bedeutet, dass Ressourcen (Drucker, CD-ROM Laufwerk usw.) mit Hilfe eines Netzwerks allen Beteiligten zur Verfügung gestellt werden können.

Datensicherung

Durch die Möglichkeit, Daten zentral zu speichern, kann auch die **Datensicherung** zentral erfolgen. Der Verlust von Daten kann so minimiert werden.

Absicherung der Verfügbarkeit von Daten

Ein Netzwerk bietet die Möglichkeit, dass bei einem Ausfall einzelner Komponenten andere Komponenten deren Aufgabe übernehmen können. So besteht die Möglichkeit, bei einem Ausfall einer Computerstation Daten und Programme von einer anderen Station abzurufen.

Optimierung der Rechnerauslastung

Stark ausgelastete Computer können durch weniger ausgelastete Stationen unterstützt werden. Dies wird häufig auch als **Lastverbund** bezeichnet.

Optimierung der Wartung

Die Möglichkeit der **Ferndiagnosen und Fernwartung** von Computersystemen über das Netz ermöglicht einen schnellen Service und vereinfachen die Administration.

3.3 Aufbauprinzipien

In einem Netzwerksystem kann die Aufteilung der Aufgaben auf zwei verschiedenen Wegen erfolgen: dem Peer-to-Peer-Netz und dem Client-Server-Konzept.

3.3.1 Peer-to-Peer-Netz

In einem Peer-to-Peer-Netz (engl. gleichgestellt) werden die Ressourcen im gesamten Netzwerk auf die beteiligten Computer aufgeteilt. Dadurch fallen keine Kosten für einen Server an. Alle Computersysteme sind gleichberechtigt und jeder Benutzer ist lokal eigenverantwortlich für die Sicherheit und die Freigabe dieser Ressourcen zuständig. Da in einem Peer-to-Peer-Netz keine zentrale Verwaltung existiert, steigt der Koordinationsaufwand mit zunehmender Netzwerkgröße enorm an.

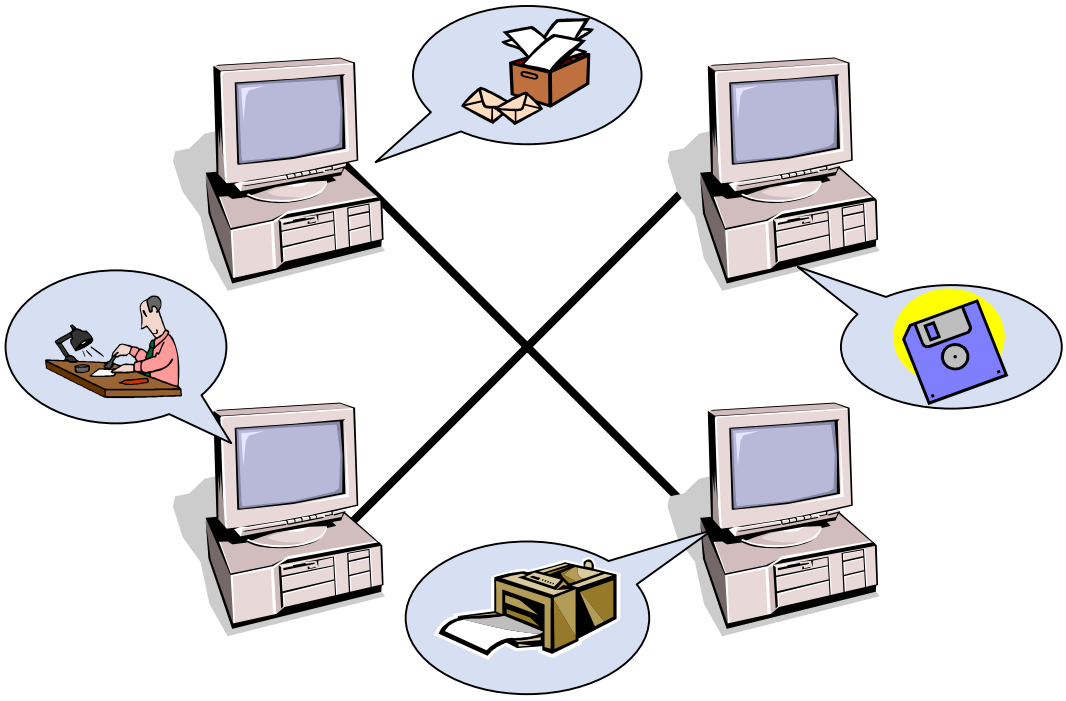

Abbildung 3-1: Peer-to-Peer Konzept

3.3.2 Client-Server

Bei einer Client-Server-Konzeption stellen ein oder mehrere Computer als Server zentral Dienstleistungen oder Ressourcen zur Verfügung. Alle anderen Computer (Clients) können nach erfolgreicher Anmeldung an den Server auf diese zugreifen. Der Client nimmt also Dienste eines Servers in Anspruch, die der Server zur Verfügung stellt. Bei größeren Netzwerken ist es üblich, Ressourcen oder Dienste auf mehrere spezialisierte Server zu verteilen. Dadurch kann jeder Server für seine spezielle Aufgabe optimal ausgerüstet werden. Mit einem Client-Server-Konzept kann eine Zentrale Benutzerverwaltung eingeführt werden, die Benutzer verschiedenen Gruppen zuordnet. Diesen Gruppen können verschiedene Rechte zugewiesen oder bestimmte Zugriffe verweigert werden. Vorteilhaft für den Benutzer ist, dass er sich von jeder beliebigen Computerstation (Client) aus unter seinem Namen im Netzwerk anmelden kann. Bestehende Peer-to-Peer-Netze können in Client-Server-Netze integriert werden. Somit schließen sich die beiden Konzepte nicht gegenseitig aus, sondern lassen sich im Bedarfsfall miteinander kombinieren. Die folgende Tabelle schildert einige der gängigsten Client-Serversysteme:

File-Server (Daten-Server)	Ein Rechner mit ein oder mehreren schnellen Festplatten dient zum Speichern aller Daten, die von den Benutzern erstellt werden. An diesem Server kann ein Gerät zur regelmäßigen Datensicherung (z.B. ein Streamer oder CD-Brenner) angeschlossen werden.
Print-Server (Drucker-Server)	Dieser Rechner stellt zentral für alle am Netz beteiligten Computer, Drucker zur Verfügung und koordiniert die Druckaufträge. Dazu wird dieser Rechner mit mehreren Anschlussstellen für Drucker ausgerüstet.
Application-Server (Anwendungs-Server)	Dieser Rechner stellt Anwendungsprogramme, die in dem ganzen Netzwerk gebraucht werden, zentral zur Verfügung. Die Benutzer starten das gewünschte Programm nicht von einer lokalen Festplatte, sondern von dieser Zentrale aus. Bei Programm-Updates muss die neue Version nur auf dem Server installiert werden und kann danach in dieser aktuellen Fassung in dem ganzen Netzwerk verwendet werden.

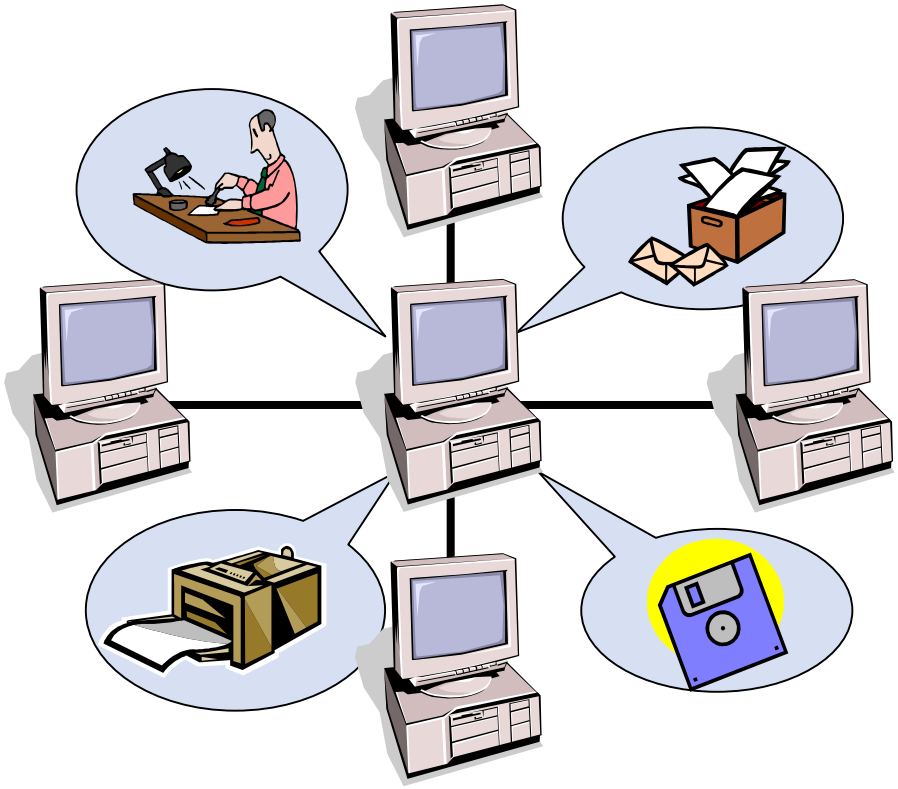

Abbildung 3-2: Client-Server Konzept

3.4 Räumliche Abgrenzung von Netzwerken

Netzwerke können nach ihrer räumlichen Ausdehnung klassifiziert werden in Local Area Network (LAN), Wide Area Network (WAN) und Metropolitan Area Network (MAN). Die Begrifflichkeiten sind nicht scharf abzugrenzen und gehen ineinander über.

3.4.1 LAN

Local Area Networks (LAN) sind auf einen begrenzten Raum (z.B. ein Gebäude) beschränkte Netzwerke mit hohen Durchsatzraten, an die unterschiedliche Hardware über unterschiedliche Schnittstellen anschließbar sind. Eine Definition der ISO (International Standards Organization) beschreibt dies folgendermaßen:

Ein lokales Netzwerk dient der Informationsübertragung zwischen miteinander verbundenen unabhängigen Geräten. Es befindet sich vollständig im rechtlichen Entscheidungsbereich des Benutzers und ist auf sein Gelände begrenzt.

3.4.2 WAN

Wide Area Networks (WAN) sind geographisch weit verteilte Netzwerke (z.B. über Kontinente). Das bekannteste WAN ist das Internet. Ihre Übertragungsraten liegen deutlich unter denen von LANs.

3.4.3 MAN

Metropolitan Area Networks sind zwischen LANs und WANs einzuordnen. Sie zeichnen sich durch die regionale Ausdehnung auf das Gebiet einer Stadt oder eines Ballungszentrums aus. Sie überbrücken dabei Entfernungen bis zu 100km.

3.5 Topologien

Die Topologie beschreibt den physikalischen Aufbau eines Netzwerkes, die Verlegung der Kabel. Die physikalische Topologie ist vergleichbar mit einer Landkarte, in der die verfügbaren Verkehrswege eingezeichnet sind. Genauso wie im Straßenverkehr, kann bei der Abwicklung des Datenverkehrs im Bereich EDV zwischen Verkehrswegen und Verkehrsregeln unterschieden werden. Die Verkehrsregeln werden logische Topologie genannt. Die logische Topologie beschreibt auf, welche Weise die Verbindungen genutzt werden. Unter anderem sind dort auch die "Zugriffsverfahren" enthalten.

Es existiert in der praktischen Umsetzung eines Netzwerkes eine sehr enge Bindung zwischen physikalischer und logischer Topologie. Im Normalfall zieht eine bestimmte physikalische Topologie eine bestimmte logische nach sich. Jedoch müssen physikalische und logische Topologie nicht identisch sein.

3.5.1 Physikalische Topologie

Die physikalische Verbindung im Netzwerk kann in verschiedenen Formen realisiert werden. Die wichtigsten Grundformen der physikalischen Topologien sind:

- Bus
- Stern
- Ring

Bus-Topologie

Die Bustopologie besteht aus einem durchgängigen Kabel. Dieses Kabel wird als Bus bezeichnet. An diesem Bus sind alle Geräte angeschlossen. Die Busenden müssen mit Endwiderständen terminiert werden, um Störungen zu vermeiden. Eine Störung des Übertragungsmediums an einer einzigen Stelle im Bus (defektes Kabel, lockere Steckverbindung, defekte Netzwerkkarte) blockiert den gesamten Netzstrang und der Datenverkehr ist unterbrochen. Dadurch gestaltet sich die Fehlersuche als sehr aufwendig, da alle Stationen überprüft werden müssen.

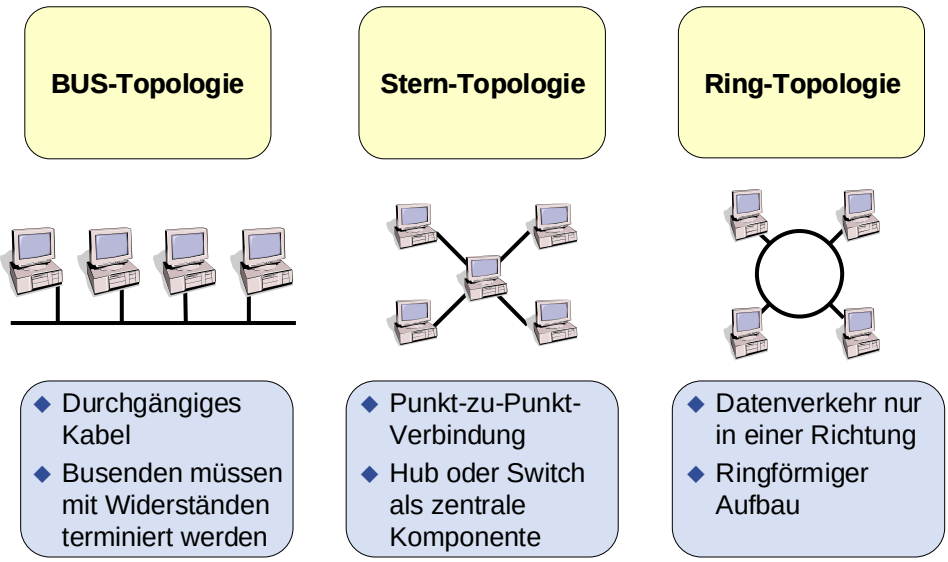

Abbildung 3-3: Physikalische Topologien

Stern-Topologie

Bei einem Stern-System sind die einzelnen Rechner mittels einer Punkt-zu-Punkt-Verbindung mit einem zentralen Verteiler verbunden. Die zentralen Komponenten können aus einem Hub oder einer Switch bestehen. Der Hub (engl. Nabe, Mittelpunkt) häufig auch als Kabelkonzentrator, Sternkoppler oder Sternverteiler bezeichnet, sendet Daten an alle Stationen des Netzwerkes, der Switch hingegen ermittelt die Zielstation und sendet die Daten nur an diese Station weiter. Bei Ausfall einzelner Kabel, fallen auch nur die jeweiligen Stationen aus, die an dem Kabel angeschlossen sind.

Ring-Topologie

Bei der Ring-Topologie bilden das Verbindungskabel eine geschlossene Form ohne Anfang und Ende. Alle Stationen werden als Elemente in diesen Ring aufgenommen. Sie verstärken und verarbeiten die Signale, die auf dem Kabel ankommen, und schicken sie weiter. Jede Station hat einen eindeutigen Vorgänger und einen eindeutigen Nachfolger. Datenverkehr findet immer nur in eine Richtung statt. Bei einem Ausfall eines Kabelteils ist der Datenstrom unterbrochen. Daher ist auch hier, wie bei der Bus-Topologie die Fehlersuche sehr aufwendig.

3.5.2 Zugriffsverfahren

Ein Zugriffsverfahren ist ein Regelwerk, das festlegt, wie die einzelnen angeschlossenen Stationen das Übertragungsmedium nutzen. Es bestimmt, wer wann senden darf. Im LAN-Bereich haben sich zwei grundlegende Zugriffsverfahren etabliert, dem CSMA/CD und dem Token Passing. Beide Verfahren verhindern Kollisionen innerhalb des Netzes. Eine Kollision entsteht, wenn zwei Netzwerkstationen gleichzeitig Daten senden, was dazu führt, dass diese Daten verloren gehen.

CSMA/CD

Bei dem CSMA/CD (Carrier Sense Multiple Access with Collision Detection) Verfahren hat jede Station jederzeit konkurrierend Zugang zum Übertragungsmedium. D.h. jede Station besitzt die gleichen Senderechte. Um Kollisionen zu vermeiden, hört die Station das Übertragungsmedium ab, bevor sie zu senden beginnt (listen before talking). Wie bei einer Gruppe wohlerzogener Menschen, die sich unterhalten möchten, beginnt eine Person ein Gespräch erst dann, wenn niemand anderes spricht. Bei einer Sendung werden die Signale in beide Richtungen des Übertragungsmediums gesendet. Kommt es zu einer Kollision von zwei Sendesignalen, da zwei Stationen das Übertragungsmedium als unbesetzt erkannt haben, stoppen die Sendestationen ihren Sendvorgang und wiederholen diesen nach einer zufällig gewählten Verzögerungszeit. Der Zeitpunkt einer Sendung kann daher nicht berechnet oder festgelegt werden. Deshalb ist dieses Verfahren ungeeignet für zeitkritische Anwendungen.

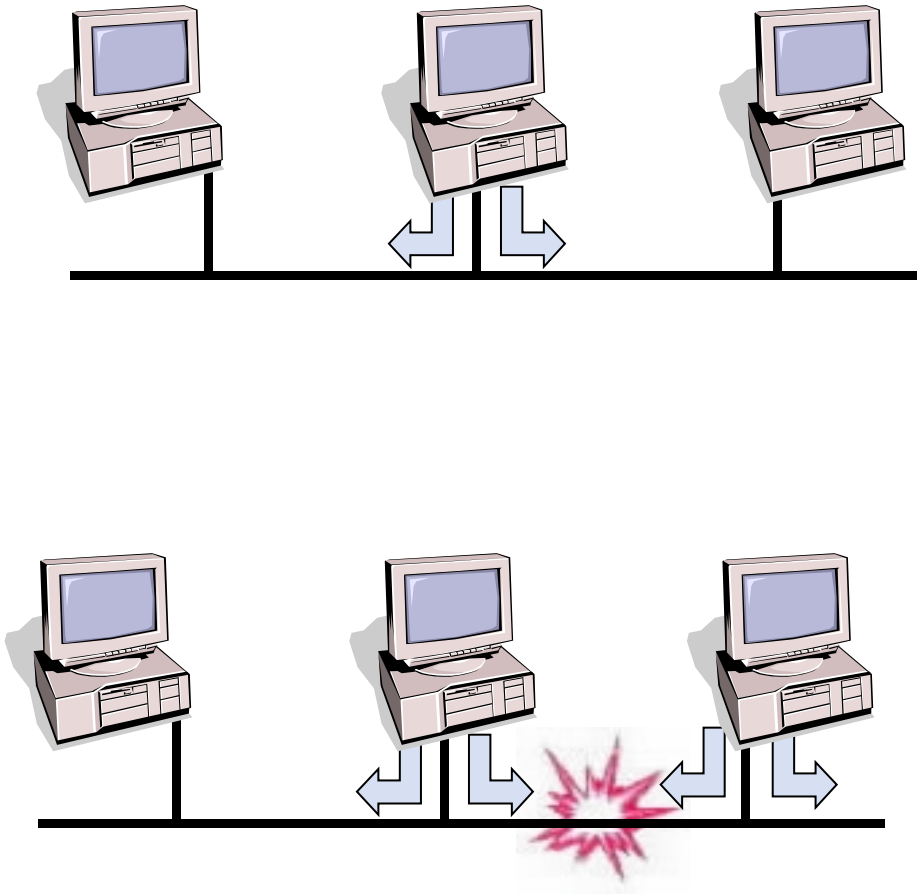

Abbildung 3-4: CSMA/CD

Token Passing

Eine Station darf erst senden, wenn sie einen sogenannten Token (engl. Zeichen) erhalten hat. Dieser Token wird vor einer Station zur nächsten weitergereicht und wird von einer besonderen Station, die die Rolle des „aktiven Monitors“ übernimmt, überwacht. Ist das Signal an der adressierten Station angekommen, wird der Erhalt der Daten quittiert, und zur Absendestation zurück gesendet. Ist diese Quittung beim Absender angekommen, wird der Token an die nächste Station weiter gereicht, die mit dem Token die Sendeerlaubnis erhalten hat. Die Kommunikation erfolgt nur in einer Richtung.

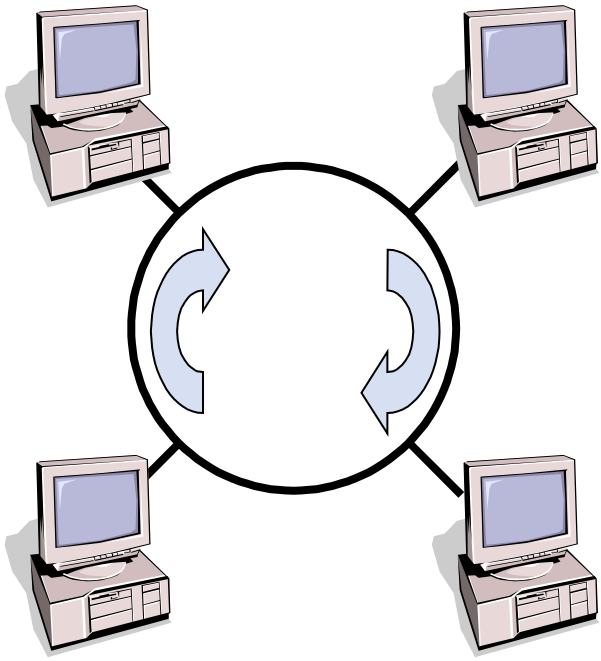

Abbildung 3-5: Token Passing

3.6 Übertragungsmedien

Datenverkehr erfolgt immer auf einem Medium. Die Medien unterscheiden sich durch ihren strukturellen und ihrem physikalischen Medium Aufbau. Grundsätzlich stehen dazu drei unterschiedliche Medien zur Verfügung:

- Metallische Leiter
- Glasfaser
- Luft

Die Übertragungsmedien können zwischen leitergebundenen (metallische Leiter, Glasfaser) und leiterungebundenen (Luft) unterteilt werden.

3.6.1 Leitergebundene Übertragung

Leitergebundene Medien werden in Form von Kabeln verlegt. Sie übertragen Informationen entweder als elektrische Impulse (metallische Leiter) oder in Form von Lichtimpulsen (Glasfaser).

Koaxialkabel

Koaxialkabel (Koax-Kabel), oder auch BNC-Kabel (Bayonet Neil-Concelman) genannt, werden für Bus-Topologien eingesetzt. Sie bestehen aus einem

Kupferinnenleiter, der von einer Isolierschicht (dielektrikum) umgeben ist. Die Abschirmung besteht aus einem Metallgeflecht oder Aluminiumfolie. Sie schützt vor elektrischen oder magnetischen Störungen.

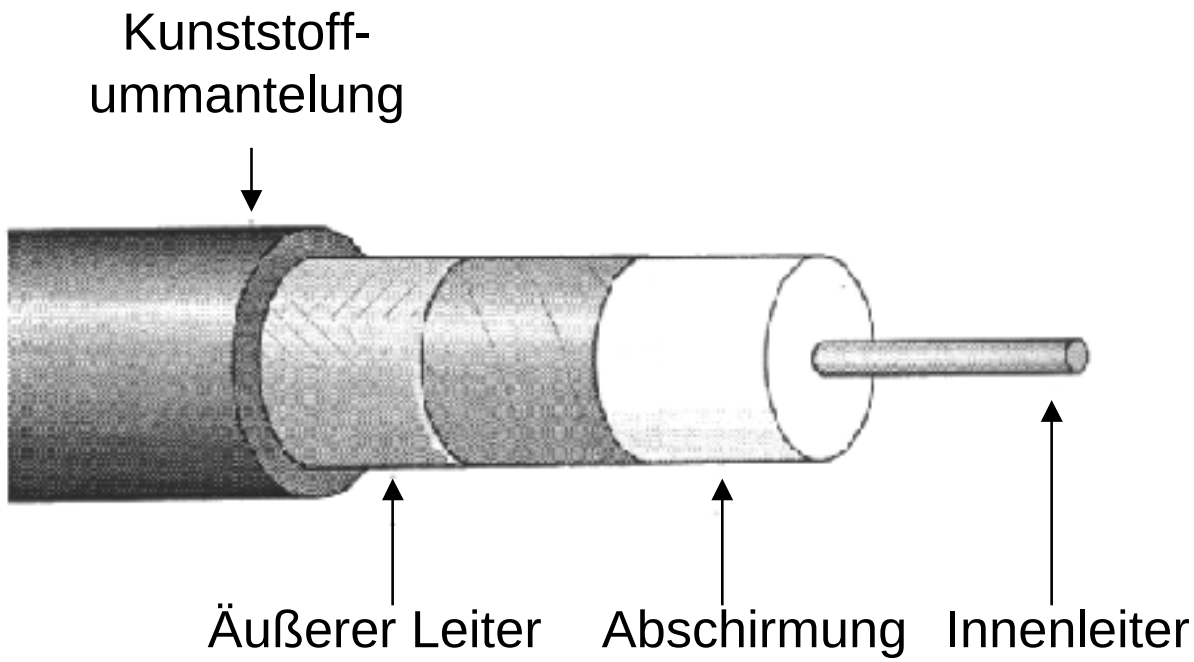

Abbildung 3-6: Koaxialkabel

Twisted-Pair-Kabel

Einfache Twisted-Pair-Kabel bestehen aus zwei isolierten Adern, die umeinander verdrillt (engl. twisted) sind. Die Verdrehung unterdrückt bis zu einem gewissen Grad Störungen von außen oder von benachbarten Aderpaaren. Twisted-Pair ist eng verbunden mit einer Stern-Topologie. Für den Anschluss an Netzwerkkarte oder Hub werden RJ-45-Stecker (Texasstecker) verwendet.

Glasfaserkabel

Glasfaserkabel, auch Lichtwellenleiter (LWL) genannt, bestehen aus einem Innenleiter aus Glas oder Kunststoff (Kern) einem Glas- oder Kunststoffmantel (Cladding) und mehreren Ummantelungen zum Schutz vor mechanischer Belastung. Der Kern besteht aus einem optisch dichteren Material (geringere Ausbreitungsgeschwindigkeit des Lichts) als der Glasmantel. Die Signalübertragung

erfolgt mittels einer Laser-Diode oder einer Lumineszenz-Diode (LED = light emitting diode). Die ausgesandten Lichtsignale werden im Inneren des Kerns durch fortlaufende Totalreflektion weitergeleitet. Ein lichtempfindlicher Empfänger wandelt die Lichtsignale auf der anderen Seite in elektrische Signale um. Die Übertragung der Signale erfolgt unidirektional. Für die Gegenrichtung wird eine zweite Faser benötigt. Glasfaserkabel sind unempfindlich gegenüber elektromagnetischer Strahlung, abhörsicher und beständig gegenüber Hitze und Witterungseinflüssen. Als problematisch erweist sich das Verbinden bzw. Verlängern der Fasern durch Verschweißen der Faserenden. Hier erfolgt eine Signaldämpfung.

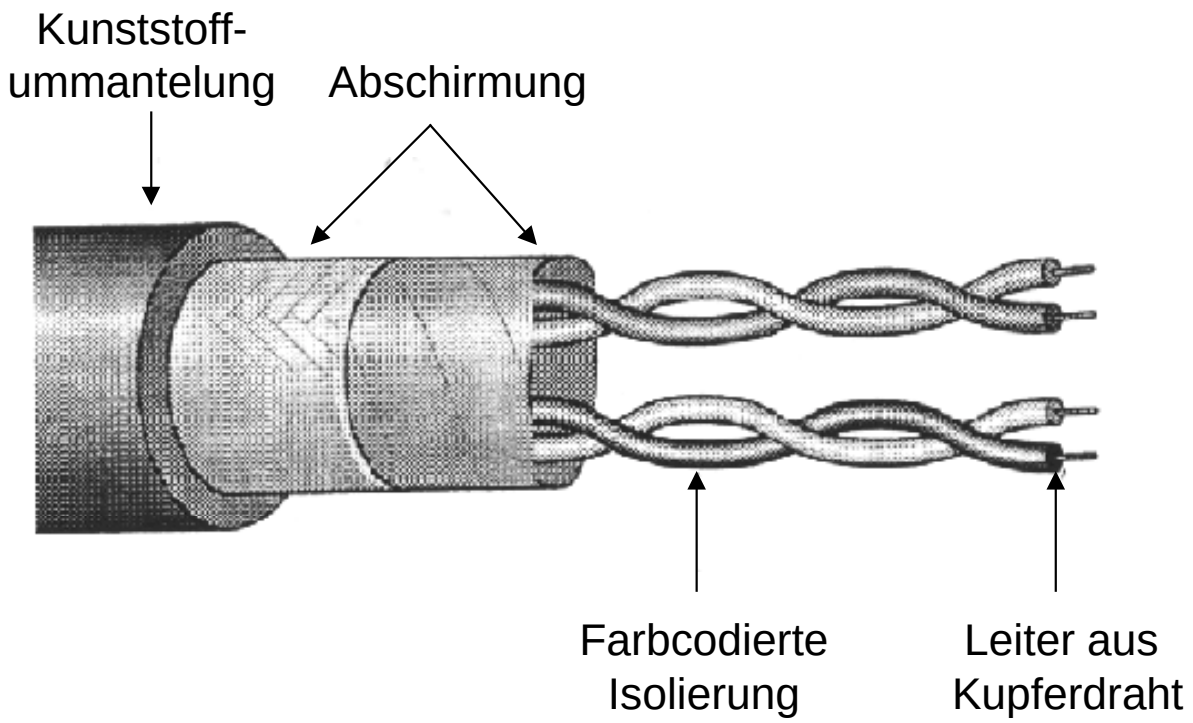

Abbildung 3-7: Twisted-Pair-Kabel

Die von Lichtwellenleitern überbrückbare Entfernung ist durch Dispersions- und Streuungseffekte begrenzt. Dispersion bedeutet, dass verschiedene Signallaufzeiten durch Lichtreflektion an den Leiterwänden dazu führen, dass die Dauer des Lichtimpulses zeitlich "gedehnt" wird. Infolge dieser Dispersion wird längs eines LWL ein Impuls zeitlich immer länger und in der Amplitude mit zunehmender Modulationsfrequenz immer kleiner. Dadurch nimmt die Bandbreite der nutzbaren Frequenz umgekehrt proportional zur Entfernung ab. Die Bandbreite ist die Spanne zwischen niedrigster und höchster zu übertragender Frequenz. Das Produkt aus

Bandbreite und Länge bildet daher eine Maßzahl, die hauptsächlich von der Art des verwendeten LWL abhängig ist. Das Bandbreiten-Längen-Produkt gibt an, bei welchen Kabellängen mit welchen Übertragungsraten gearbeitet werden kann. Bei einem Bandbreiten-Längen-Produkt von 1 GHz x km kann

- bei 500 m Länge mit einer Bandbreite von 2 GHz gearbeitet werden.
- bei 1 km Länge mit einer Bandbreite von 1 GHz gearbeitet werden.
- bei 2 km Länge mit einer Bandbreite von 500 MHz gearbeitet werden.

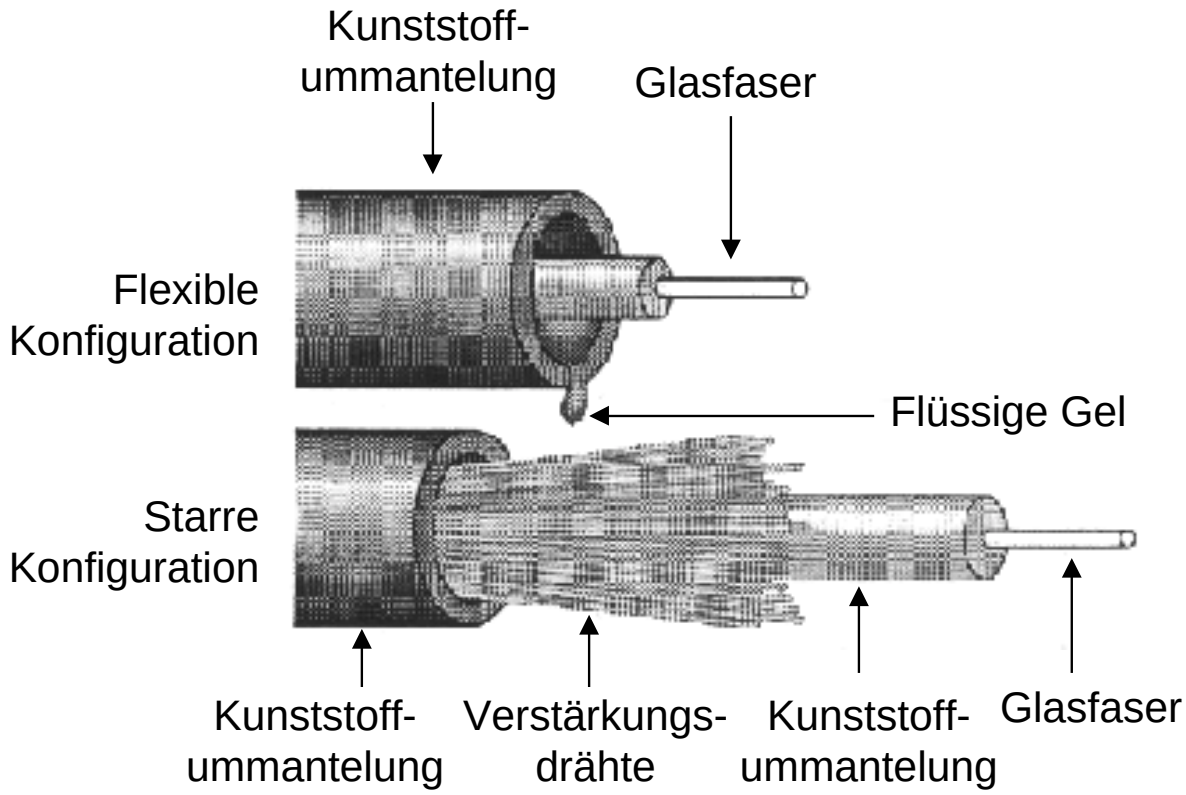

Abbildung 3-8: Glasfaserkabel

3.6.2 Leiterungebundene Übertragung

Bei der leiterungebundenen oder auch drahtlosen Übertragung werden Funksignale anstelle von Kabeln verwendet. Sie kann entweder als Punkt-zu-Punkt-Kommunikation z.B. zur Überwindung von großen Distanzen mit Hilfe von Richtantennen erfolgen, oder als Mehrpunkt-Kommunikation. Bei der Mehrpunkt-

Variante werden so genannte Access-Points eingesetzt, die im Prinzip wie ein Hub funktionieren und mit einem festen Netz verbunden werden können.

Wesentliche Nachteile der drahtlosen Übertragungsverfahren sind die geringen Datenübertragungsraten und die mangelnde Sicherheit gegenüber Abhören. Weiterhin werden die maximal überbrückbaren Distanzen von den geografischen Gegebenheiten bestimmt.

Zusammenfassende Übersicht Kabel

Kabel	Koaxial	Twisted-Pair	Glasfaser
Kosten	mittel	niedrig	hoch
Übertragungsraten	10 Mps	1 bis 155 Mps	2 Gps (üblich 100 Mps)
Dämpfung	niedriger als Twisted-Pair	hoch	am niedrigsten
Reichweite	einige km	einige 100 Meter	einige 10 km
Störanfälligkeit für elektromagnetische Einflüsse	weniger empfindlich als Twisted-Pair	empfindlicher als Koaxial	keine

Tabelle 3-1: Übersicht Kabel

3.7 OSI-Referenz-Modell

Um eine herstellerunabhängige, freie Kommunikation zwischen Systemen (z.B. Rechner oder einem Rechnerverbund) zu ermöglichen, müssen genormte Regeln für den Informationsaustausch festgeschrieben und eingehalten werden. Das Open-System-Interconnection kurz OSI-Referenzmodell ist ein genormtes Architekturmodell für Kommunikationssysteme, welches die Übermittlung von Daten zwischen zwei Systemen logisch aufteilt.

Es legt folgendes fest:

- Hierarchische Gliederung der notwendigen Kommunikationsaufgaben in sieben Schichten,

- festlegen der Aufgaben der einzelnen Schichten und
- festlegen der Protokolle zur Kommunikation zwischen Schichten gleicher Ebene.

3.7.1 Sieben Schichten des OSI-Referenzmodells

In dem folgenden Bild sind die sieben Schichten des OSI-Referenzmodells dargestellt.

Nr	OSI-Schicht	Aufgaben
7	Application-Layer (Anwendungs-Schicht)	Anwendungen
6	Presentation-Layer Darstellungs-/Präsentations-Schicht)	Datenformate, Darstellungs-, Verschlüsselungsfunktionen
5	Session-Layer (Kommunikationssteuerungs-/Sitzungs-Schicht)	Verbindungen, Flusskontrolle (Kommunikationsparameter), Datenfluß-Prüfpunkte
4	Transport-Layer (Transport-Schicht)	Pakete, Flusskontrolle, Fehlerbehandlung und Empfangsbestätigung
3	Network-Layer (Vermittlungs-/Netzwerk-Schicht)	Adressinformationen, Routing
2	Data Link-Layer (Sicherungs-/Datenverbindungs-Schicht)	Frames, Fehlerbehandlung
1	Physical-Layer (Bitübertragungs-Schicht)	Definition physikalischer Werte

Tabelle 3-2: OSI-Referenzmodell

1. Physikal-Layer (Bitübertragungs-Schicht)

In der Bitübertragungsschicht werden die binären Signale übertragen. In dieser Schicht werden die elektrischen Funktionen, die Übertragungsverfahren und das Übertragungsmedium festgelegt.

2. Data-Link-Layer (Sicherungs-/Datenverbindungs-Schicht)

Diese Schicht stellt eine zuverlässige Informationsübertragung durch den geordneten Zugriff auf das Übertragungsmedium und Strukturierung der Daten sicher.

3. Network-Layer (Vermittlungs-/Netzwerk-Schicht)

Die Vermittlungsschicht realisiert eine Verbindung zwischen den kommunizierenden Stationen über verschiedene Netzwerkknoten hinweg und legt dadurch den optimalen Verbindungsweg im Netz fest.

4. Transport-Layer (Transport-Schicht)

Die Transport-Schicht transportiert die Nachrichten von einem Endsystem zum anderen. dazu werden die notwendigen Transportverbindungen errichtet, gesteuert und beendet.

5. Session-Layer (Kommunikationssteuerungs-/Sitzungs-Schicht)

Die Kommunikationssteuerungsschicht steuert die so genannten Sitzungen. Sie legt Regeln fest und überwacht diese für den Datenaustausch. Weiterhin werden Synchronisationspunkte festgelegt, an denen bei Problemen der Datenaustausch wieder aufgenommen werden kann.

6. Presentation-Layer (Darstellungs-/Präsentations-Schicht)

In der Darstellungs-Schicht werden die Daten in ein allgemeines Standartformat konvertiert. Weitere Aufgaben sind die Komprimierung und Verschlüsselung der Daten.

7. Application-Layer (Anwendungs-Schicht)

Die Anwendungsschicht beschreibt die Schnittstelle, über die Anwendungen auf Dienste eines anderen Systems zugreifen können.

3.8 Protokolle

Ein Protokoll ist eine Menge von Regeln und Konventionen zwischen Teilnehmern eines Kommunikationsprozesses (nach STEVENS). Ein einzelnes Protokoll ist immer nur für eine Teilaufgabe zuständig. daher werden mehrere Protokolle zu Protokollsammlungen zusammengefasst, den so genannten Protokoll-Stacks (engl. Stapel). Eine Kommunikation zwischen zwei Stationen funktioniert nur dann, wenn

sie den gleichen Protokoll-Stack benutzen, oder wenn Geräte eingesetzt werden, die zwischen verschiedenen Stacks vermitteln können.

3.8.1 TCP/IP

Das Transmission Control Protocol/Internet Protocol kurz TCP/IP ist heute das Standardprotokoll für Netzwerksysteme. Es wird sowohl im LAN-Bereich als auch im Internet-Bereich verwendet.

Das Transmission Control Protocol/Internet Protocol kurz TCP/IP geht von einem vierschichtigen Architekturmodell aus.

Schicht	TCP/IP	OSI
4	Anwendungs-Schicht	Application-Layer
		Presentation-Layer
		Session-Layer
3	Transport-Schicht (TCP)	Transport-Layer
2	Internet-Schicht	Network-Layer
1	Netzwerk-oder Link-Schicht	Data-Link-Layer
		Physical-Layer

Tabelle 3-3: TCI/IP Protokoll

Die grundlegenden Charakteristika der Protokolle sind:

- Unabhängigkeit von physischen Übertragungsmedien,
- Offene Standards, die unabhängig von spezieller Hardware oder bestimmter Betriebssysteme sind.
- weltweiter einheitlicher Adressierungsmechanismus
- Standards in der Anwendungsebene

Nachfolgend ist eine Liste mit Diensten angeführt, die in der Protokollfamilie TCP/IP zusammengefasst sind.

Protokoll	Name	Beschreibung
TCP	Transmission Control Protocol	Verbindungsorientiertes Protokoll zur sicheren Datenübertragung, das logische Verbindungen zwischen Applikationen aufbaut.
UDP	User Datagramm Protocol	Transportprotokoll, im Gegensatz zu TCP ungesicherter Transport
IP	Internet Protocol	Paketvermittler über IP-Adressen
FTP	File Transfer Protocol	ermöglicht den Datenaustausch über Netzwerk
HTTP	Hypertext Transfer Protocol	dient dem Transport von HTML-Seiten (Hypertext Markup Language)
SMTP	Simple Mail Transfer Protocol	Protokoll zum versenden von E-Mails
DNS	Domain Name Service	setzt Domainnamen in IP-Adressen um (und umgekehrt)

Tabelle 3-4: Dienste

3.8.2 Port-Nummer

Da auf einem System gleichzeitig mehrere Dienste über TCP mit gleicher IP-Adresse ablaufen können, muss über eine zusätzliche Kennung deutlich gemacht werden, welcher dieser Dienste konkret benötigt wird. Dies erfolgt über die so genannte Port-Nummer oder Dienstnummer, die jedem einzelnen Dienst eine spezifische Nummer zuordnet. Somit wird ein Dienst im Netzwerk eindeutig identifizierbar: Diese

Kombination aus IP-Adresse und Port-Nummer ist ein so genannter Socket, der Endpunkt einer Datenübertragung im Netzwerk.

3.9 Schnittstellen

Eine Schnittstelle (Interface) bezeichnet den Ort, an dem verschiedene Hard- und/oder Softwarekomponenten miteinander kommunizieren. Schnittstellen können in vier verschieden Arten eingeteilt werden:

- Hardwareschnittstelle, das Verbindungsglied zwischen verschiedenen Hardwarekomponenten
- Softwareschnittstelle, zum Datenaustausch zwischen verschiedenen Programmen
- Benutzerschnittstelle, zur Eingabe von Daten durch den Benutzer
- Programmierschnittstelle, ermöglicht das Ausführen von Funktionen innerhalb des Betriebssystemes

Der Anschluss peripherer Geräte an einen Computer erfolgt durch die Hardwareschnittstelle. Damit eine Datenübertragung möglich ist, müssen Datensignale hinsichtlich ihrer physikalischen Eigenschaften so gewählt sein, dass sie der jeweilige Empfänger aufnehmen und verarbeiten kann. Die Hardwareschnittstelle definiert die Festlegung für die physikalischen Eigenschaften der Schnittstellenleitungen. Die Spezifikation einer Schnittstelle muss folgendes enthalten:

- Schnittstellenleitungen
- Stecker/Buchse
- Belegung

Ein aktueller Standard-PC besitzt in der Regel drei verschiedene externe Schnittstellen zur Kommunikation mit Peripherie-Geräten, die serielle, die parallele Schnittstelle und der USB (Universal Serial Bus). Die Übertragung der Daten erfolgt, wie in der Bezeichnung angegeben, seriell oder parallel. Für die serielle Übertragung steht nur eine Leitung zur Verfügung, über die die Bits nacheinander (seriell) übertragen werden. Die Anschlüsse der seriellen Schnittstelle werden als COM-Ports (COM=Communication, Port=Anschluß) bezeichnet. Bei der parallelen Übertragung

können mehrere Bits, in der Regel acht, als ein komplettes Byte, über parallele Leitungen transportiert werden. Normalerweise besitzt ein PC einen parallelen Anschluss, der als LPT1 (Line Printer 1) bezeichnet wird und für einen Drucker vorgesehen ist. Eine Weiterentwicklung der externen Schnittstellen ist der USB. Obwohl der USB von der Namensgebung her ein Bus sein müsste, ist er als kombinierte Stern-Bus-Struktur ausgelegt. An der Spitze steht der USB-Hostadapter im Computer, an dem bis zu 127 Geräte angeschlossen werden können. Die Datenübertragung erfolgt über ein bidirektionales Leitungspaar.

In der Industrie werden spezielle Bussysteme zur Übertragung von Daten und zur Kommunikation verwendet. Als Beispiele seien hier drei verschiedene Schnittstellen zur Kommunikation vorgestellt:

CAN-Bus (Controler Area Network)

CAN ist für die serielle Datenübertragung in einer Bus-Topologie ausgelegt. Als physikalisches Medium wird die Zweidrahtleitung verwendet. Als Zugriffsverfahren verwendet der CAN-Bus CSMA/CA (Carrier Sense Multiple Access with Collision Avoidence). Dieses Verfahren baut auf dem CSMA/CD auf, es arbeitet mit einer zusätzlichen Regel zur Vermeidung von Kollisionen (collision avoidence). Die sendewillige Station sendet eine Warnmeldung aus, die bewirkt, dass die anderen Stationen warten. Die Haupteinsatzgebiete sind in der Automobilindustrie zu finden.

Profibus (Prozess Field Bus)

Als Übertragungsmedium ist eine Zwei-Drahtleitung vorgesehen, es kann aber auch ein Lichtwellenleiter verwendet werden. Der Zugriff wird über Token Passing geregelt. Wird ein Fehler durch einen fehlerhaften Aufruf oder gestörte Antwort festgestellt, muss der Aufruf wiederholt werden.

SERCOS-Interface (Serial Real Time Communication System)

Das SERCOS-Interface ist eine Schnittstelle für geschlossene Regelkreise. Die Hauptanwendungsgebiete sind Steuerungen von Servo-Antrieben bei Werkzeugmaschinen durch nummerische Steuerungen. Der Datenaustausch erfolgt über Lichtwellenleiter.

4 Internet

4.1 Geschichte des Internets

Das Internet und hier besonders das World Wide Web (WWW) ist nicht nur das jüngste, sondern auch das am rasantesten wachsende Massenmedium.

Ein Datum für den Beginn der Vorbereitung eines Computernetzes kann nicht genau festgelegt werden.

So könnten zum Beispiel die Straßen- und Kommunikationssysteme der Chinesen, Perser, Assyrer, Römer und Mongolen als antike Vorbilder angesehen werden. Die Nachrichtenübermittlung wurde dabei von Boten übernommen, die zwischen festgelegten Distanzen verkehrten. Ein weiterer Vorläufer des Internets ist der Telegraph. Durch ihn konnten die Menschen seit 1836 Nachrichten über weite Strecken schnell übermitteln. Die Übermittlung erfolgte durch nur zwei verschiedene Zeichen: kurze und lange Striche. Zusätzlich sind die Pausen zwischen den Signalen ausschlaggebend. Der Computer übermittelt Daten ebenfalls im binären System, nur die Zeichen sind andere als die von 1836. Der Computer "versteht" ausschließlich die Zeichen "0" und "1".

1876 erfand Alexander Graham Bell das Telefon. Bis heute sind Telefonleitungen das wichtigste Datentransportmittel im Internet.

Die historische Entwicklung im engeren Sinn geht auf die Arbeitsgruppe ARPA (Advanced Research Projects Agency zurück, die vom amerikanischen Verteidigungsministerium 1958 gegründet wurde. Die Amerikaner, geschockt durch den sowjetischen Vorsprung bei der Raumfahrt („Sputnik-Schock“), überlegten ein Kommunikationsnetz einzurichten, welches auch bei größeren Ausfällen noch funktionieren würde. Die Leitung der Arbeitsgruppe übernahm Joseph Carl Robnett Licklider. Licklider war ein Visionär, der schon frühzeitig erkannte, dass Computer nicht nur zu rein wissenschaftlichen Zwecken genutzt werden sollten, sondern in Zukunft dank interaktiver und intuitiver Bedienung immer größere Verbreitung finden würden. Dazu gehörte seiner Meinung nach auch die Vernetzung von Computerpower und er unterstützte viele Pionierprojekte in diese Richtung.

1966 wurde die Idee geboren, die ARPA-eigenen Rechner zu vernetzen und somit einzelne Großrechneranlagen kostengünstig allen angeschlossenen Rechnern zugänglich zu machen

1969 wurde zunächst das ARPANET gegründet, welches vier Forschungseinrichtungen über gemietete Telefonleitungen miteinander verband. Die Systemplattformen waren erstmals zueinander inkompatibel. Die Lösung für die Kommunikation lag in einem IMP (Interface Message Processor), der als Zwischenglied zwischen Netzwerk und Rechner diente.

Das erste Übertragungsprotokoll im APRANET war NTP (Network Transfer Protocol), dass eine paketorientierte Übertragung vornahm. Eine Datei wird beim Absender in viele kleine Päckchen zerlegt. Jedes Päckchen enthielt unter anderem Absender- und Ziel-Adresse und wurde einzeln von IMP zu IMP übertragen, die Route wurde je nach aktueller Leitungstopologie von jedem IMP autark bestimmt.

Die ersten Dienste im APRANET waren TELNET (zur Steuerung entfernter Rechner) und FTP (zur Datenübertragung). Trotzdem fehlte noch eine interaktive Kommunikationsplattform, die 1971 durch Erfindung der E-mail (Electronic mail) geschlossen wurde.

Da der Datenverkehr rasant zunahm, war das NTP-Protokoll den Anforderungen nicht mehr gewachsen und es wurde das leistungsfähigere TCP (Transmission Control Protocol) eingeführt, das zunächst auch die Adressierungen im Netz vornahm. Erst 1980 wurde für die Adressierung das IP (Internet Protocoll) eingeführt.

Um den Kommunikationsaustausch der nicht nur APRA abhängigen Forschungseinrichtungen zu gewährleisten wurde das CSNET (Computer Sience Network) eingeführt, dass ab 1984 allen Fachbereichen der Universitäten offenstand.

Ein weiterer, wichtiger Schritt zum universellen Kommunikationsnetz war die Entwickung des Dienstes *Gopher*: Gopher ermöglichte es, reine Textdateien hierarchisch auf einem Server anzulegen und herunterzuladen. Doch erst ein anderer Dienst eröffnete das Internet für die breite Öffentlichkeit: Das WWW.

Genau diesen Gedanken hatte der Brite Tim Berners-Lee, damals Informatiker am »CERN«, dem Institut für Teilchenphysik in Genf, als er im März 1989 einen neuartiges Hypertextsystem für das hauseigene Intranet vorschlägt: Das *World Wide Web* bietet eine gut durchdachte Bedienoberfläche, die mit speziellen Programmen, den *Browsern* angezeigt werden kann.

Besonders hervorstechend sind die Fähigkeiten Text, Grafik, Töne und Videos zu multimedialen Präsentationen zu verbinden. Eine weitere Neuerung stellen die *Hyperlinks* dar, mit denen aus jedem WWW-Dokument zu einer anderen Ressource im Internet verwiesen werden kann. Erstmals ist es möglich, ohne größeres Fachwissen einen Dienst zu bedienen und eigene Informationen aufzubereiten und im Internet zu veröffentlichen.

4.2 Aufbau des Internets

Das Internet ist die Gesamtheit aller (durch verschiedene Netzwerktechniken) vernetzten Computer, also auch Netzwerke mit unterschiedlichen Protokollen. Wenn vom WWW gesprochen wird handelt es sich lediglich um einen Teil dieses Verbundes, nämlich ein Hypermedia-System, das einen Teil der Internetprotokolle für sich nutzt. Es werden heute viele Begriffe genannt, wenn über das Internet oder WWW gesprochen wird, Server, Protokolle, Provider, Modem sind nur einige. Im Folgenden sollen nun wesentliche Funktionszusammenhänge erklärt werden. Zunächst soll die grundsätzliche Topologie des Internets erläutert werden. Wie sieht die physische Vernetzung aller Rechner aus?

Dazu gibt es die sogenannten **Carrier**, spezielle Anbieter, die ein eigenes Netzwerk betreiben und kleineren Providern, eine Anbindung an sein Netz ermöglicht. Der **Provider** (Anbieter, Bereitsteller) stellt seinen Kunden, meist dem Endverbraucher die Einwahl zum Internet zur Verfügung.

4.2.1 Backbones

In Abbildung 4-1 ist schematisch das Backbone (Backbone = Rückgrat) eines Carriers mit zwei angeschlossenen Providern dargestellt.

Provider A betreibt einen PoP (**P**oint **o**f **P**resence = Einwahlknoten) mit vier angeschlossenen Computern. Er selbst ist über ein Backbone des Carriers an das Internet angebunden. Für diesem Zweck beherbergt Provider A einen Schaltschrank des Carriers, der als Gegenstelle für die Backbone-Verbindung zum Provider B dient.

Provider B betreibt einen PoP, in unserem Beispiel mit fünf angebundenen Rechnern. Der Carrier betreibt hier ebenfalls einen Schaltschrank, der zum einen die Verbindung nach »außen« ins Internet gewährleistet, aber auch zum Provider A.

Das Rechenzentrum des Provider B ist nun über eine weitere Verbindung (in der Grafik dicker als die Verbindung zwischen Provider A und B, da sie nun den

Datenverkehr für zwei Provider verkraften muss) an ein sogenanntes *CIX* (**C**ommercial **I**nternet E**x**change = Kommerzieller Internet-Austauschpunkt) angebunden, das eine neutrale Austauschstelle als Übergang zu anderen Carriernetzwerken darstellt. Siehe zu diesem Thema auch den nächsten Punkt.

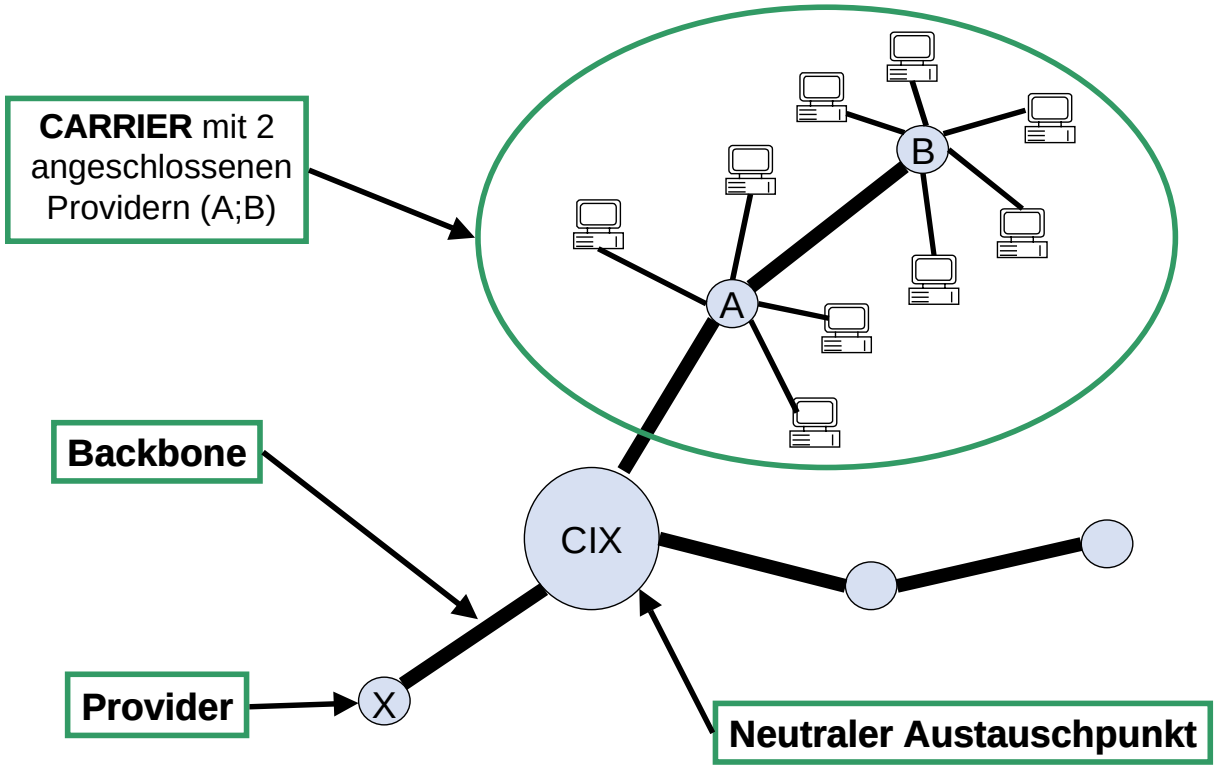

Abbildung 4-1: Aufbau Internet

4.2.2 Neutrale Austauschstellen

Ein neutraler Austauschpunkt (engl. *Peering-Point*) ist ein zentraler Übergang zwischen eigenständigen Netzwerken von Carriern (Abbildung 4-1). Solche zentrale Austauschstellen zwischen Providern existieren, um teure Leitungskosten einzusparen, da auf die Weise nicht jeder Provider eigene Leitungen zu anderen Providern betreiben muss und die interkontinentalen Verbindungen geschont werden, da der meiste nationale Datenverkehr so auch national abgewickelt werden kann.

Eingerichtet ist ein CIX in der Regel in einem Rechenzentrum, in das jeder Provider seine eigene Leitung hineinführt. Innerhalb dieses Rechenzentrums endet dann jede providereigene Leitung in einem providereigenen Router (im nebenstehenden Beispiel die Carrier-Router), die dann wiederum innerhalb CIX an ein zentrales Hausnetz angeschlossen sind, in dem dann der eigentliche Datenaustausch (das

sogenannte *Peering* = »gleichstellen«) zwischen den einzelnen Providern anhand komplexer Routing-Tabellen erfolgt.

Für die neutralen Austauschpunkte gibt es mehrere Begriffe, die sich meistens nach der Größe, Bedeutung und Standort des jeweiligen Austauschpunktes richten. Der bedeutendste, neutrale Austauschpunkt in Deutschland ist z.B. das *DECIX* in Frankfurt am Main. Des weiteren gibt es noch einen kleineren Austauschpunkt in München, das sogenannte *INXS*. In anderen europäischen Staaten gibt es eigene, nationale Austauschpunkte. So z.B. in Großbritannien das *LINX* , in Wien das *VIX* usw..

In den USA gibt es in den größeren Metropolen eigene neutrale Austauschpunkte. Darüber hinaus gibt es sogenannte *MAE* (»**M**etropolitan **A**rea **E**xchange«), die überregional innerhalb der USA neutrale Austauschpunkte betreiben.

4.3 Funktionsweise des Internets

Das Internet ist ein sehr großes, weltumspannendes, dezentrales Netzwerk. In einem dezentralen Netzwerk sind die Verbindungen zwischen den Computern nach keinem fixen Schema angeordnet, es gibt auch keine Zentralrechner.

Um von Punkt A zu Punkt B zu gelangen, gibt es viele unterschiedliche Wege. Ein Ausfall von Computern oder Verbindungen legt nicht das Netz lahm, Daten können über eine alternative Strecke übertragen werden.

Die einzelnen Netze oder Computer sind über das Protokoll TCP/IP (Transfer Control Protocol/Internet Protocol) miteinander verbunden. TCP/IP ist ein Standard für die Datenübertragung, der es erlaubt, Rechner unterschiedlichen Typs miteinander zu verbinden.

4.3.1 Verbindung zum Internet

Es gibt zwei prinzipiell verschiedene Arten sich mit dem Internet zu verbinden:

1. Einwahlverbindung

Wenn ein Computer ausschließlich als Client fungiert, ist es nicht nötig, dass er ständig mit dem Internet verbunden ist. Es reicht dann eine Verbindung zu einem entfernten Computer, etwa Mail- oder Webserver aus, welcher wiederum permanent mit dem Internet verbunden ist. Dieses kann zum Beispiel vom heimischen Rechner

mit einem Modem oder einer ISDN-Karte erfolgen. Hierzu sind spezielle Protokolle notwendig.

2. Permanente Verbindung

Wenn ein Computer selber als Server fungieren soll, also Dienste oder Daten für andere bereitstellen soll, ist eine permanente Verbindung notwendig, da es für gewöhnlich nicht absehbar ist, wann auf einen Server zugegriffen wird.

4.3.2 Adressierung durch IP-Adressen

Bei einer Verbindung zum Internet braucht jeder Computer eine genaue Identifizierung. Diese wird durch die sogenannten IP-Adressen erreicht. Diese bestehen aus einer 32 Bit-Zahl, werden jedoch wegen der besseren Verständlichkeit für den Menschen in Punktiert-dezimaler Schreibweise dargestellt. Sie werden in vier sogenannte **Quads** zu je 8 Bit unterteilt, jeder dieser Quads wird dabei durch einen Punkt getrennt. Am besten lässt sich diese Adressierung durch ein Beispiel verdeutlichen: Angenommen es soll eine Verbindung zu einem Rechner im Otto-Klüsener-Haus (OK-Haus) an der Universität Hannover aufgebaut werden. Die IP-Adresse könnte dann wie folgt lauten: 130.75.178.10

Dezimal	**130.**	**75.**	**178.**	**10**
Quads	**1**	**2**	**3**	**4**
Binär	10000010	01001011	10110010	00001010

Tabelle 4-1: Dezimale und binäre Schreibweise der IP-Adressen

Die Punkte haben die Aufgabe untergeordnete Netze anzusprechen. So wie zu einer Telefonnummer im weltweiten Telefonnetz eine Landeskennzahl, eine Ortsnetzkennzahl, eine Teilnehmerrufnummer und manchmal auch noch eine Durchwahlnummer gehört, gibt es auch im Internet eine Vorwahl - die **Netzwerknummer (NN)**, und eine Durchwahl - die **Hostnummer (HN).** Deshalb werden die Netze in Klasse A-Netze, Klasse B-Netze und Klasse C-Netze aufgeteilt.

Quad / Klasse	1	2	3	4
A-Netz	NN	HN		
B-Netz	NN		HN	
C-Netz	NN			HN

Tabelle 4-2: Netzklassen

Für Klasse A-Netze werden beim ersten Quad die Nummern 1-126 vergeben, die letzten drei Quads sind vom Netzbetreiber frei verfügbar. Es gibt also maximal 126 solcher Netze. Das amerikanische Militärnetz ist ein Beispiel für ein Klasse A-Netz.

Klasse B-Netze sind für das erste Quad alle Zahlen von 128-192 möglich, die Zahl des zweiten Quad liegt zwischen 0-255. Dadurch sind 16384 solcher Netze möglich. Die letzten beiden Zahlen der IP-Adresse sind auch hier frei verfügbar, so dass an dieses Netz 65536 Hostrechner angeschlossen werden können. Beispiel für Klasse 2-Netze sind große Firmen, Universitäten oder Online-Dienste.

Bei Klasse C-Netzen liegt die Zahl des ersten Quads zischen 192 und 223. Die Zahlen der nächsten beiden Quads gehören ebenfalls noch zu den Netzwerknummern. Da für den letzten Quad nur noch 256 Zahlen übrigbleiben, können in einem C-Netz maximal 256 Hostrechner angeschlossen werden.

Bei dem gegeben Beispiel mit der „Uni-Adresse“ handelt es sich also um eine Klasse B-Netz mit folgender Adressierung:

Die ersten beiden Quads (130.75) bezeichnen die Netzwerknummer, in diesem Fall die Universität Hannover.

Die 178 und die 10 kennzeichnen die Hostadresse, wobei die 178 für das OK-Haus steht und die 10 einen Rechner im OK-Haus bezeichnet.

4.3.3 Domain Name Service (DNS)

Hinter dem Domain Name Service (DNS) verbirgt sich ein System, welches das unüberschaubare Zahlensystem der IP-Adressen in anschauliche Namensadressen übersetzt. Die Namen werden in umgekehrter Reihenfolge als die IP-Adressen gelesen. Ein Beispiel für eine Adresse nach dem DNS-System ist : www.uni-

hannover.de. Nach diesem System vergebene Adressen, werden als **Uniform Resource Locator (URL)** bezeichnet.

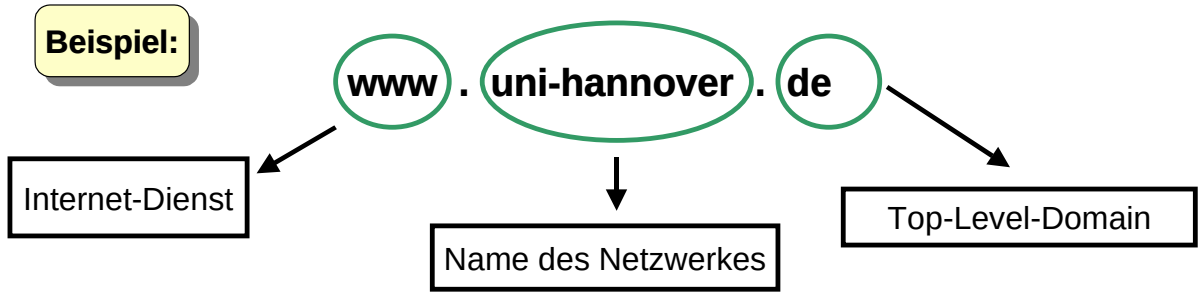

Abbildung 4-2: Beispiel DNS-Adresse

„WWW“ steht für den Internet-Dienst, „uni-hannover“ ist der Name des Netzwerkes (Universität Hannover) und das „de“ am Ende bezeichnet den Gebietsstandort Deutschland. Das „de“ am Ende der Adresse wird auch als „Country-TOP-Level-Domain“ (cTLD) bezeichnet. Neben den Länderkennzahlen gibt es noch Top-Level-Domains nach Themengebieten geordnet, die so genannten „Generic Top Level Domains“ (gTLD)

Zunächst wurden nur die TLD der Kategorien, wie zum Beispiel .com oder .net eingeführt. Da diese Domains nicht ausreichten, wurden neue TLD für jedes Land eingerichtet. Verwaltet werden diese Domains den Network Information Center (NIC). Für Deutschland ist es der DENIC, wo jede „de“-Adresse beantragt und eingetragen werden muss.

Country Top-Level-Domain (cTLD)	Land
.de	Deutschland
.uk	United Kingdom
.us	United States
Ca. 250 weitere	

Generic Top Level Domains (gTLD)	Kategorie
.arpa	Einrichtung des ARPANet nur systeminterne Nutzung
.com	„commercial“ Kommerz
.edu	„education“ Bildungsorganisationen
.org	„organization“ Nicht-Kommerzielle Org.
Weitere, .net, .int, .mil, ...	

Tabelle 4-3: Top-Level Domains

Der mittlere Teil der DNS-Adresse, in unserem Fall „uni-hannover“, bezeichnet das Netzwerksystem. Diese Domain kann durch Punkte weiter in Subdomains unterteilt werden. Beispiel hierfür wäre: www.ok-haus.uni-hannover.de oder www.ifw.uni-hannover.de. Eine weitere Unterteilung ist häufig auf nationaler Ebene durch ein zusätzliches Kurzzeichen zum Beispiel „.gov“ für government zu finden. Bei solch einer Domain www.wien.gov.at spricht man von einer nationalen Level 3-Domain.

4.3.4 Datenübertragung im Internet

Verschiedene Dienste (Datenarten)

Als Dienst wird eine Funktion des Internets bezeichnet. In der OSI-Terminologie ist er eine besondere Fähigkeit oder Funktionensammlung einer Schicht, die diese einer übergeordneten Schicht am so genannten Dienstzugangspunkt anbietet. Ein Dienst wird immer der direkt übergeordneten Schicht angeboten. Die Dienste der einzelnen Schichten werden von den unterschiedlichen Aufgaben dieser Schichten geprägt. Der Dienst e-Mail hat beispielsweise die Funktion, Nachrichten von einer Person zu einer anderen Person zu schicken. Dieser Dienst muss in einem Protokoll (Kapitel 3.8) geregelt werden, damit die Nachrichten von allen Nutzern standardisiert empfangen und versendet werden können. In diesem Protokoll werden alle technischen Dinge, die den jeweiligen Dienst betreffen, geregelt. Das WWW ist

beispielsweise auch ein Dienst, ein anderer ist z.B. Telnet. Alle Dienste werden über Ports am Rechner angesprochen. Bekannte Dienste und Protokolle sind:

- **E-Mail (Dienst)-** zum Versenden beliebiger Nachrichten an bekannte Empfänger. Alles was vom Empfänger bekannt sein muss, ist seine E-Mail-Adresse, damit ihm Nachrichten geschickt werden können. Das zugehörige Protokoll ist SMTP (Simple Mail Transfer protocol) zum Senden der Nachrichten.
- **Telnet (Dienst und Protokoll)**- zum Steuern eines anderen Rechners im Netz.
- **File Transfer (FTP) (Dienst und Protokoll)** - zum Übertragen von Dateien und Dateiverzeichnissen.
- **Gopher (Dienst und Protokoll)**- zur Datenabfrage. Dieser Dienst war der Vorläufer des WWW und ist heute schon veraltet.
- **Chat (IRC) (Dienst und Protokoll)** - zum Online-Tratsch mit anderen Teilnehmern.
- **Newsgroups (News)** - zur öffentlichen Diskussion im Usenet. Jeder Usenet-Teilnehmer kann Beiträge veröffentlichen, welche weltweit gelesen werden können.
- **World Wide Web (Dienst)** - zum bequemen Aufsuchen von Informationen. Das WWW ermöglicht dem Benutzer auch ohne technische Kenntnisse - hauptsächlich per Mausklick - sich auf veröffentlichten Seiten zurechtzufinden und mittels Verweisen auf andere Dokumente (sogenannte Hyperlinks oder kurz "Links") zu anderen Seiten zu finden. Diese Links können auf irgendein Datenelement auf irgendeinem beliebigen Rechner im Internet zeigen. Grundgerüst der Dokumente im WWW ist HTML (Hypertext Markup Language). Das zugehörige Protokoll ist HTTP.

Ablauf der Datenübertragung im WWW

Um den Weg und die Art der Datenübertragung im Internet zu verstehen, soll an dieser Stelle ein Beispiel im WWW zur Verdeutlichung herangezogen werden.

Zunächst gibt man in die Adresszeile des **Browsers** oder auch **Client** genannt**,** die gewünschte Zieladresse ein, zum Beispiel www.uni-hannover.de . Ein Browser ist ein Programm, das verwendet wird, um auf Web-Server zuzugreifen um heruntergeladene Dokumente darzustellen. Die beiden am weitesten verbreitetsten Browser sind der Netscape Navigator und der Microsoft Internet Explorer.

Bedingung ist nun eine Verbindung zum Internet, wie in Kapitel 4.3.1 beschrieben und das auf dem entfernt liegendem Host-Server die richtige Server-Software installiert ist (WWW, FTP, Gopher, E-mail, etc.). In diesem Fall muss es ein WWW-Server sein. Bei Eingabe der Adresse, schickt der eigene Rechner nun eine Anfrage an den Host-Server, natürlich mit dem Absender, der eigenen IP-Adresse. Da die gewünschte Seite in der Programmiersprache **HTML** (Hypertext Markup Language) geschrieben ist, benötigt der Datentransfer ein passendes Protokoll, um den zu übertragenen Seiten das richtige Datenformat zuweisen zu können. In diesem Fall ist dies **HTTP** (Hypertext Transfer Protocol). **Hypertext** bedeutet, dass in einem Dokument vorkommende Begriffe eine Verbindung zu einer anderen Datei aufweisen können, auf der Browseroberfläche durch die sogenannten „Hyperlinks“ oder nur „links“ zu erkennen. Nun werden die Daten, in kleine Pakete aufgeteilt, basierend auf dem OSI-Schichtenmodell (Kapitel 3.7), durch verschiedene Schichten geleitet.

Wenn die anwendungsorientierten Schichten durchlaufen sind, kommt es zu der eigentlichen Datenübertragung der einzelnen Pakete. Bei Modemeinwahl gibt es ein spezielles Protokoll, das für die „Modemstrecke“ zuständig ist, das PPP (Poin To Point Protocol). Jedes dieser Pakete bekommt eine Adressierung mit der Ziel-IP-Adresse. Der Transport wird durch das TCP geregelt, die Adressierung durch das IP (Kapitel 3.8).

Die Pakete, die mit Hilfe des TCP-Protokolls gesendet werden, gelangen nun zum Beispiel über Modem zum Provider. Dort werden sie am Host-Server entgegengenommen und weitergeleitet zu der Zieladresse. Diese Aufgabe wird von sogenannte **Routern** erledigt. Diese sind notwendig, da das Internet aus einer Anzahl von Netzwerken besteht, die in irgendeiner Form miteinander kommunizieren müssen. Der Router weiß anhand der adressierten Datenpakete in welche Richtung der Transport der Pakete weitergeleitet werden muss. Er ist also eine Art

„Vermittlungsstelle“. Ist bei der Einwahl per Modem dem ersten Router die Adresse nicht bekannt, wird das Datenpaket zum nächsten Router weitergeleitet. Dieses wiederholt sich solange bis die Zieladresse erreicht ist. Es kann also passieren, dass ein Datenpaket, das von einem nahegelegenem Rechner abgerufen werden soll, sehr große Strecken zurücklegt.

4.4 Information im Internet

Die Informationsverbreitung durch das Internet in den letzten Jahren rasant zugenommen. War es früher sehr mühselig schnelle Information über bestimmte Fachgebiete zu bekommen, so genügen heute häufig schon ein paar Mausklicks. Im Zuge der Informationsverbreitung über das Internet wird i.d.R. das WWW als der Dienst mit dem größten Informationsgehalt genannt. Durch die Anzahl der Beteiligten in diesem Netzwerk ergeben sich für die Suche nach Informationen eine Menge Vorteile aber auch Probleme.

1. Wie gelange ich zu den gewünschten Informationen?

   Im Prinzip gibt es nur zwei Möglichkeiten: Entweder ist die gewünschte Zieladresse bekannt, oder es ist eine Seite bekannt hinter der sich gewünschte Daten befinden (links). Die andere Möglichkeit, und das ist i.d.R. die häufigere, ist das Suchen und Finden von Informationen mit Hilfe von Suchmaschinen. Eine Suchmaschine kann man mit einem wissenschaftlichen Buch vergleichen. Um in so einem Buch schnell etwas zu finden, schaut man im Stichwörterverzeichnis nach. Eine **textorientierte Suchmaschine** sucht in ihrer Datenbank auch nach den eingegeben Stichwörtern ("Keywords") und liefert die Seiten als Ergebnis, die zu den Stichwörtern passen. Die Keywords in der Datenbank der Suchmaschine bekommt sie von den einzelnen Websites, nach denen Sie ständig im WWW auf der Suche ist. Diese Aufgabe übernehmen die sogenannten Spider-Programme oder auch „Robots“.

   Indexorientierte Suchmaschinen besitzen ein Verzeichnis mit einer Vielzahl von Rubriken. Jeder Teilnehmer mit einer eigenen Webseite kann sich unter der entsprechenden Rubrik bei dieser Suchmaschine anmelden und auch gefunden werden.

   Heute besitzen nahezu alle Suchmaschinen diese beiden Arten der Informationsbeschaffung (www.yahoo.de, www.google.de, etc.). Zusätzlich gibt es noch Meta-Suchmaschinen, die keine eigenen „Robots“ besitzen, sondern Ihre

Ergebnisse von einer Vielzahl andere Suchmaschinen bekommen und sich sozusagen die besten Ergebnisse heraussuchen. (www.metager.de, www.metacrawler.de) Die Relevanz der Ergebnisse und die Quelle der Information werden dem Benutzer angezeigt

Der Anwender gibt also in die Adresszeile des Browser die Adresse einer Suchmaschine ein (z.B. www.google.de, oder www.yahoo.de, etc.) und kann dort in einem Fenster den gesuchten Begriff oder mehrere Begriffe eingeben. Das Ergebnis der Suche sind Webseiten, in denen dieser Begriff vorkommt. Die Reihenfolge der Suchergebnisse ist von den enthaltenen Schlüsselwörtern sowie der Anzahl der Aufrufe einer Seite abhängig.

2. Welche Informationen sind relevant?

Das WWW bietet zwar eine fast unbegrenzte Menge an Informationen, die für einen selbst relevanten Informationen sind jedoch häufig schwieriger zu finden. Das Problem, das global jeder eigene Informationen im WWW bereitstellen kann, führt bei der Informationssuche schnell zu einer unübersichtlichen Datenmenge. Es gibt auch keine Garantie für den Wahrheitsgehalt der gefundenen Informationen. Häufiges Problem ist auch die gesammelten Datenmengen für sich so aufzubereiten, dass dadurch „Wissen“ entsteht, wie es in Kapitel 2.1 problematisiert wurde.

3. Verschiedene Länder mit verschiedenen Rechten

Da nahezu alle Länder der Erde Teil des Netzwerkes „Internet“ sind, war schon zu Beginn der 90er Jahre die Diskussion über den „rechtsfreien Raum“ Internet vorhanden. Inhalte, die beispielsweise in Deutschland verboten sind, können in anderen Ländern frei verfügbar und legal sein. Dieses Problem ist bis heute nicht gelöst.

5 Sicherheit

Das Problem der Sicherheit im Internet und in lokalen Netzwerken ist heute sehr schwerwiegend und verursacht immense Schäden. Im Folgenden sollen einige bekannte Sicherheitsprobleme erläutert werden. Dazu soll eine Unterscheidung zwischen äußerer (z.B. Viren) und innerer (z.B. fehlender Passwortschutz im LAN) Sicherheit gemacht werden. Gleichzeitig soll vorgestellt werden, wie dieser Bedrohung entgegen getreten werden kann, also welche wirksamen Schutzmaßnahmen es gibt.

5.1 Sicherheit gegen Zugriff (Datenschutz)

5.1.1 Sicherheitslücken nach außen (z.B. Viren)

a) Computerviren

Definition: Ein Computervirus ist eine Befehlsfolge, die ein Wirtsprogramm zur Ausführung benötigt. Die Ausführung eines Virus bewirkt, dass eine Kopie (Reproduktion) oder eine modifizierte Version des Virus in einen Speicherbereich, der diese Befehlssequenz noch nicht enthält, geschrieben wird (Infektion). Zusätzlich zur Fähigkeit zur Reproduktion enthalten Viren in der Regel einen Schadensanteil. Dieser kann unbedingt oder bedingt durch einen Auslöser aktiviert werden.

Aufbau und Funktion: Ein Virus besteht aus einer Virenkennung und einem Infektionsteil sowie optional aus einem Schadens- und einem Sprungteil. Durch die Ausführung des Infektionsteils kopiert sich ein Virus in einen Speicherbereich. Handelt es sich dabei um den in einer Datei gespeicherten Code eines ausführbaren Programms, so werden i.d.R. die Strukturinformationen des infizierten Programms durch die Angabe der neuen Dateilänge sowie durch Veränderung der Einsprungadresse angeglichen. Die neue Einsprungadresse entspricht der Anfangsadresse des Virus-Codes. Soll nach der Ausführung des Virus doch noch das Programm mit der ursprünglichen Funktionalität ausgeführt werden, so enthält der Virus-Code im optionalen Sprungteil eine Rücksprungadresse, die die Einsprungadresse in das ursprüngliche Programm ist.

Anhand einer speziellen Virenkennung kann ein Virus in seiner Infektionsphase erkennen, ob ein Programm schon vom Virus befallen ist. Dies verhindert das

wiederholte Infizieren von Programmen. Diese Viren-Kennung dient im Gegenzug Virenerkennungsprogrammen zur Aufdeckung von infizierten Programmen.

Die Ausführung des Schadensteils kann von Randbedingungen abhängig gemacht werden. Dies kann beispielsweise ein besonderes Datum sein, an dem die Schadensfunktion startet (z. B. das Formatieren der Festplatte).

Viren-Verbreitung: Mit dem Einzug des Personal Computers in den 80er Jahren und einer dezentralisierten Verwaltung isoliert betriebener PCs, verbreiteten sich die Viren der „ersten Generation“ hauptsächlich über das Kopieren von Daten von Diskette zu Diskette oder die manuelle Installation von Programmen auf einzelnen PCs. Da es aber noch keine globales Netzwerk wie das Internet in seiner heutigen Form gab, war dieses Problem relativ leicht in den Griff zu bekommen. Viren der „zweiten Generation“ verbreiten sich über die Öffnung der Systeme nach außen, also durch eine flächendeckende weltweite Vernetzung von Rechnern.

Viren-Typen:

Die Viren der **ersten Generation** waren hauptsächlich Programm- und Boot-Viren. Ein Programm-Virus kopiert sich in eine ausführbare Datei. Nach der Infektion liegt ein ausführbares Programm vor, das beim Aufruf zunächst den Virus und dann erst das eigentliche Programm ausführt. Zur Verschleierung des Virus wurden auch die Strukturdaten der infizierten Dateien verändert.

Boot-Viren befallen die Bereiche einer Diskette oder Festplatte deren Datei beim Hochfahren des Rechners, also beim Systemstart, gelesen und in den Hauptspeicher geladen werden. Der Bootsektor enthält das Ladeprogramm, durch dessen Ausführung das Betriebsystem in den Hauptspeicher geladen und ausgeführt werden kann. Ein Boot-Virus wird meist vor dem Bootsektorprogramm in den Speicher geschrieben, so dass beim Hochfahren des Systems zunächst der Virus ausgeführt wird.

Viren der **zweiten Generation** verbreiten sich durch offene Systeme und stellen heute eines der zentralen Probleme der Netzwerksicherheit dar. Es ergibt sich eine neue Vielzahl an Kanälen, über die fremde Code-Stücke auf den lokalen Rechner gelangen können. Beispiel für solche Kanäle sind E-Mails, Java-Applets, elektronische Dokumente oder auch Postscrip-Dateien. Auch die Verbesserung heutiger Software-Werkzeuge trägt erheblich zur Verbreitung von Viren bei. Diese zunächst wenig einleuchtende These lässt sich jedoch einfach mit der zunehmenden

Automatisierung von Vorgängen beider Informationsverarbeitung begründen. Wesentliches Ziel der entwickelten Werkzeuge ist es, möglichst viele Aktivitäten automatisch und transparent für den Benutzer durchzuführen. Diese eigentlich höchst wünschenswerte Eigenschaft hat jedoch für den Virenbereich fatale Konsequenzen. Unter Nutzung von Werkzeugen wie Postscript-Interpretern, Textverarbeitungsprogrammen oder MIME (Multipurpose Internet Mail Extension → E-Mail-Anhang) werden fremde Codebausteine oder fremde Dokumente automatisch ausgeführt und die darin enthaltenen Viren werden transparent für den Benutzer, also ohne dessen explizites Eingreifen, in Umlauf gebracht.

a) Makro-Viren

Ab Mitte 1995 machte sich bei Computer-Viren ein neuer Trend bemerkbar, der durch die zunehmende Verbreitung von grafisch orientierten Bedienungsoberflächen (wie z. B. Windows) unterstützt wird. Waren unter den zeichenorientierten Betriebssystemen (z.B. MS-DOS u.ä.) Daten- und Programmdateien sauber getrennt, so gestatten neuere Programme in einer grafischen Umgebung Datendateien mit umfangreichen Steuerinformationen wie z. B. Makros für häufig benötigte Steuerungsaufgaben. Damit ist nun keine saubere Trennung zwischen Daten und Programmroutinen mehr möglich. Im Gegensatz zu konventionellen DOS-Viren kann die Verbreitung daher auch über Datendateien geschehen. Jede z.B. über elektronische Post (E-Mail) verschickte Nachricht kann direkt oder als "Anhang" ("attachment") infiziert sein und durch "Anklicken" aktiviert werden. In der Praxis hat diese Bedrohung insbesondere bei den Dateien der Programme Word für Windows (WINWORD) und EXCEL (und inzwischen auch ACCESS) der Firma Microsoft seit dem Jahre 1996 weltweit beträchtlich zugenommen. Die Word-Makro-Viren haben inzwischen die Spitzenstellung bei gemeldeten Infektionen eingenommen. Interessant zu bemerken bleibt noch, dass die Makro-Viren auf verschiedenen Betriebssystem-Plattformen auftreten können, nämlich allen, auf denen WINWORD läuft (Microsoft Windows und Windows für Workgroups der Versionen 3.1 und 3.11, Windows 95/98, Windows NT, Macintosh).

Gegenmaßnahmen:

Die Gegenmaßnahmen zur Virenbekämpfung lassen sich in zwei Klassen einteilen:

- Präventive Virenabwehr (Administrative Maßnahmen)
- Werkzeuge zur Erkennung eines Virenbefalls

Zu den Präventivmaßnahmen zählen die Konfiguration von Rechnern, das Beschränken von Schreibberechtigungen, das Verschlüsseln von Daten, die Verwendung digitaler Fingerabdrücke, das Impfen von Programmen sowie administrative Maßnahmen zur Abwehr von Makroviren.

Die am häufigsten eingesetzten Werkzeuge gegen Viren sind die Viren-Scanner. Bekannte Viren besitzen eine Virenkennung oder enthalten spezifischen Bytemuster bzw. Codesequenzen, woran sie erkannt werden können. Einfache Virenscanner durchsuchen Programme auf das Vorhandensein dieser Merkmale hin und zeigen die gefundenen Viren an. Auf diese Weise können natürlich nur bereits bekannte Viren erkannt werden. Mutierende oder neue Viren schlüpfen durch das Netz dieser Scanner. Aus diesem Grund suchen einige Erkennungsprogramme anhand von Heuristiken (versuchsweise Annahmen, Hypothesen) auch unbekannte Viren zu entdecken. Die Heuristiken suchen nach verdächtigen Codesequenzen in Programmen, die auf Virenaktivität hindeuten, wie z.B. Befehle die dem Suchen nach neuen Opfern und dem Kopieren/Replizieren des Virus entsprechen. In Anbetracht der rasanten Entwicklung und Verbreitung neuer Viren ist auf jeden Fall eine regelmäßige Aktualisierung der Viren-Erkennungsprogramme unerlässlich.

b) Würmer:

Ein Wurm ist ein ablauffähiges Programm, das sich vervielfältigt. Ein Wurm-Programm besteht in der Regel aus mehreren Programmteilen, den Wurm-Segmenten. Die Vervielfältigung erfolgt selbständig unter Kommunikation mit anderen Wurm-Segmenten. Die Verbreitung von Würmern erfolgt insbesondere über ein Netzwerk, indem sich der Wurm auf andere Rechner innerhalb des Netzes kopiert. Die ausführbaren Programmteile können den Quellcode eines Programms beinhalten, der auf dem zu überfallenden Rechner übersetzt werden muss, sie können aber auch direkt in ausführbarer Maschinensprache oder interpretierbarer Sprache, z.B. Shell-Kommandos geschrieben sein. Durch Würmer treten Bedrohungen der Integrität und Vertraulichkeit, aber auch Bedrohungen der Verfügbarkeit auf, die sogenannten „Denial-of-Service“ Angriffe. Würmer beanspruchen i.d.R. viele Ressourcen, da sie bei ihrer Verbreitung über das Netzwerk eine sehr hohe Netzlast erzeugen und durch einen möglichen Mehrfachbefall von Rechnern deren Speicherressourcen ausschöpfen können.

Beispiel: Einer der bekanntesten Würmer ist der ILOVEYOU-Wurm vom Mai 2000. Dieser führte in zuvor kaum gekannter Geschwindigkeit zum Zusammenbruch der elektronischen Datenverarbeitung in vielen europäischen und amerikanischen

Firmen und Behörden. Man schätzt den verursachten Schaden auf 10 Milliarden Euro. Es handelt sich um einen Wurm, der als .vbs-Datei (Visual Basic Script) über E-Mail Attachements verbreitet wurde, in deren Betreffzeile ILOVEYOU stand. Die Verbreitung des Wurms setzte eine Microsoft Windows-Ungebung voraus, da der Wurm sich der Daten von Windows Outlook bediente, um eine Mail mit dem Wurm als Attachement an die in der Adressdatei gespeicherte Mailadressen zu senden. Der Wurm zerstört gezielt Dateien des lokalen Datensystems, die u.a. JPEG-Bilder, MP2- oder MP3 Musik-Daten oder Videodateien enthielten. Schließlich durchsuchte der Wurm auch die lokale festplatte nach Passworten und versuchte, eine Verbindung aufzubauen, um diese Daten an den Programmierer des Wurms zu übermitteln. Durch diese Schadensfunktion stellt ILOVEYOU eine wesentlich größere Bedrohung als der im März 1999 aufgetretene E-Mail Wurm Melissa. Melissa verbreitete sich ebenfalls unter Nutzung der Outlook Adressdatei und hat allein in den USA einen materiellen Schaden von 80 Millionen Dollar verursacht.

Gegenmaßnahmen: Im Gegensatz zu Viren, die sich meist auf „legalem“ Weg verbreiten, versuchen Würmer Bugs und Lücken in System-, und Anwendersoftware auszunutzen. Durch eine restriktive Vergabe von Zugriffsberechtigungen, lässt sich ein unerlaubtes Akquirieren von Informationen und das Einbringen von fremden Code beschränken. Besonders Passwortdaten sind so zu schützen, dass nicht jeder Benutzer Leserecht darauf erhält. Generell sind differenzierte und restriktive Rechtefestlegungen und Kontrollen notwendig, insbesondere bei Zugriffen von entfernten Rechnern, Die fehlende differenzierte Zugriffskontrolle in den Windows Betriebssystemen, Windows 95, 98, hat ursächlich dazu beigetragen, dass sich der ILOVEYOU-Wurm in einer bis dahin noch nicht bekannten Geschwindigkeit ausbreiten konnte.

c) Trojanisches Pferd

Das trojanische Pferd in der Sage beschreibt die Charakteristika von Programmen, die als Trojanische Pferde bezeichnet werden sehr genau: es wird eine Funktionalität vorgetäuscht, die Vertrauen erweckt, die aber auch durch eine verborgene, bedrohliche Funktionalität ergänzt wird.

Definition: Ein Trojanische Pferd ist ein Programm, dessen implementierte Ist-Funktionalität nicht mit der angegebenen Soll-Funktionalität übereinstimmt. Es erfüllt zwar diese Soll-Funktionalität, besitzt aber eine darüber hinausgehende, beabsichtigte zusätzliche Funktionalität.

Ein Trojaner besteht in der Regel aus mehreren Komponenten. Das Server Programm, der Client, und Konfigurationstools. Das Serverprogramm ist der Teil, der verschickt wird, und sich auf dem "feindlichem Rechner" installiert. Mit dem Client kann der Hacker auf den Server zugreifen. Bei der Konfiguration gibt es meist mehrere Möglichkeiten. Der Server wird so eingestellt, dass nur die Personen auf den PC zugreifen können, die das Passwort kennen, oder es wird so konfiguriert, das der Server jedem antwortet.

Ein Trojanisches Pferd besitzt also verborgene Eigenschaften, um z.B. in ein System einzudringen, um Daten aufzuzeichnen oder zu manipulieren. Auf Benutzerebene wird dabei korrektes Verhalten vorgetäuscht. Trojanische Pferde können mit dem Programmstart aktiviert oder durch spezielle Auslöser, wie beispielsweise das Eintreten eines bestimmten Datums, gestartet werden. Man spricht hierbei von einer logischen Bombe.

Trojanische Pferde können in ganz unterschiedliche Bereichen eines Systems auftreten. Beispiele dafür sind Editoren oder Textverarbeitungsprogramme, die die Inhalte edierter Dateien unbemerkt und unautorisiert kopieren. Weitere Beispiele sind manipulierte Datenbanken, durch die sensible Informationen zum Angreifer durchsickern können, oder auch manipulierte Betriebssystemfunktionen, durch die der Angreifer beispielsweise zusätzliche Zugriffsrechte erhält.

Beispiel: Ende März 1998 gelang es zwei Schülern aus Köln auf sehr einfache Weise, 6000 Passwörter von T-Online Kunden zu knacken. Dazu entwickelten sie kleine Werkzeugprogramme, die T-Online Power Tools, deren Soll-Funktion darin bestand, einige Verwaltungsaufgaben zu automatisieren und zu erleichtern. Diese Programme waren über das Internet frei verfügbar. Bei deren Verwendung wurden die Benutzer gebeten, sich bei den Autoren registrieren zu lassen. Dies ist eine durchaus übliche Vorgehensweise, um Nutzer über Updates, Bugs etc. zu informieren. Die Tools waren jedoch ein Trojanisches Pferd, dessen zusätzliche Funktionalität darin bestand, die Festplatte des Opfers nach verschlüsselt abgelegter Zugangsdaten des T-Online-Dienstes zu durchsuchen. Mit der Registrierung wurden diese Daten dann unbemerkt für den Benutzer an die Angreifer übermittelt. Die Angreifer profitierten dabei von der Bequemlichkeit von solchen Benutzern, die ihre Zugangsdaten nicht jedes Mal neu eingeben, sondern auf Festplatte speichern. Unter Nutzung einer speziellen Software war es dann trivial, die unter Windows verschlüsselten Passworte zu entschlüsseln.

Gegenmaßnahmen: Sensible Daten, wie Passworte, PINs und TANs sollten möglichst nicht auf Speichermedien, wie Festplatte gespeichert werden, auf die ungehindert lesend zugegriffen werden kann. Ist ein Angreifer im physischen Besitz einer Festplatte, z.B. durch Diebstahl eines Notebooks, so ist es ein leichtes, das installierte Betriebssystem durch booten von MS-DOS zu umgehen und direkt auf den Speicher zuzugreifen. Werden dennoch sensible Daten gespeichert, so sind starke kryptographische Verfahren zu deren Verschlüsselung einzusetzen (folgende Kapitel).

Generell sollte der Wirkungsgrad eines Benutzers beschränkt sein um seine Manipulationsmöglichkeiten zu minimieren. Jeder sollte nur die notwendigen Zugriffsrechte erhalten. Weiter Möglichkeit ist der Einsatz von digitalen Unterschriften in Programmen, welche vor Programmstart überprüft wird.

d) Sicherheitslücken von TCP/IP

Das sogenannte Adress-Spoofing ist einer der häufigsten Angriffe im Internet. Dabei „maskiert“ sich der Angreifer, er baut unter gefälschter Identität eine Verbindung auf und benutzt zum spionieren die Absenderadresse des angegriffenen Rechners. Gerade e-commerce Anbieter sind ein beliebter Angriffspunkt für Adress-Spoofing, großes Aufsehen erregte die Lahmlegung der Web-Portale von Yahoo, Amazon oder eBay Anfang 2000.

e) Sicherheitslücken im WWW

Auch im WWW gibt es eine Reihe von Schwachstellen in der Sicherheit, die von Hackern ausgenutzt werden können. Als Beispiel sollen hier die sogenannten „Cookies“ erläutert werden. Cookies sind Informationen in ASCII-Text, die durch die aufgerufene HTML-Datei generiert (z.B. per Java-Script) und dem Browser zum Ablegen auf der lokalen Platte übergeben werden. Ein Cookie kann also nur das "tun", was der Browser zulässt. Und das ist bei modernen Browsern relativ wenig: Es können nämlich nur die Dinge abgefragt werden, die von dem Browser in den speziell für Cookies reservierten Bereich hineingeschrieben worden sind. Der primäre Sinn eines Cookies ist, Informationen auf die lokale Festplatte zu schreiben, sodass bei einem erneuten Aufruf einer Webseite individuelle Präferenzen oder auch Passwörter gleich erscheinen. Cookies passen also das Netz an die Bedürfnisse des Einzelnen an, um dessen Arbeit zu erleichtern.

Die Gefahren von Cookies liegen darin, dass die Privatssphäre eingeschränkt wird, da andere Server auch auf diese Cookies zugreifen können und somit gewisse persönliche Vorlieben oder Neigungen öffentlich werden können.

Das Verhindern von Cookies ist recht simpel. Die Funktion der Cookies lässt sich im Browser ohne Schwierigkeiten abstellen, es sind dann jedoch viele angenehme Funktionen nicht mehr möglich

f) E-mail: SMTP hat kein Verschlüsselung

Das Problem von E-Mail liegt in dem Protokoll, dass zum Versenden der Nachrichten dient SMTP. SMTP verfügt über keine Verschlüsselungsfunktion, sodass alle Mails unverschlüsselt übertragen und auf Vermittlungsrechnern offen zwischengespeichert werden. Da Datenleitungen generell abgehört oder zwischengespeicherte Mails modifiziert werden können, sind sie im hohem Maß Angriffen auf ihre Vertraulichkeit und Integrität ausgesetzt.

Um dies zu vermeiden dient eine Verschlüsselung. Diese kryptographische Verfahren werden im nächsten Kapitel erläutert.

g) weitere Sicherheitslücken:

Die Gefahr der in den vorhergehenden Abschnitten beschriebenen Sicherheitslücken stellt nur einen kleinen Teil potenzieller Sicherheitsattacken dar. Generell lässt sich zusammenfassen, dass sämtliche Dienste, wie WWW, Telnet, **E-mail**, etc. und der dazugehörenden Protokolle, durch die Öffentlichkeit und den freien Datentransfer im

Internet Sicherheitslücken aufweisen. Aus diesem Grund sind grundlegende Gegenmaßnahmen im Folgenden Kapitel dargestellt.

Allgemeine Gegenmaßnahmen

a) Kryptographische Verfahren

Unter Kryptographie wird die Lehre von den Methoden zu Ver- und Entschlüsselung von Nachrichten zum Zweck der Geheimhaltung von Informationen gegenüber Dritten verstanden. Unterschieden wird heute zwischen symmetrischen und asymmetrischen Verfahren:

Die sicher naheliegendste Form der Verschlüsselung ist die **symmetrische Verschlüsselung**.

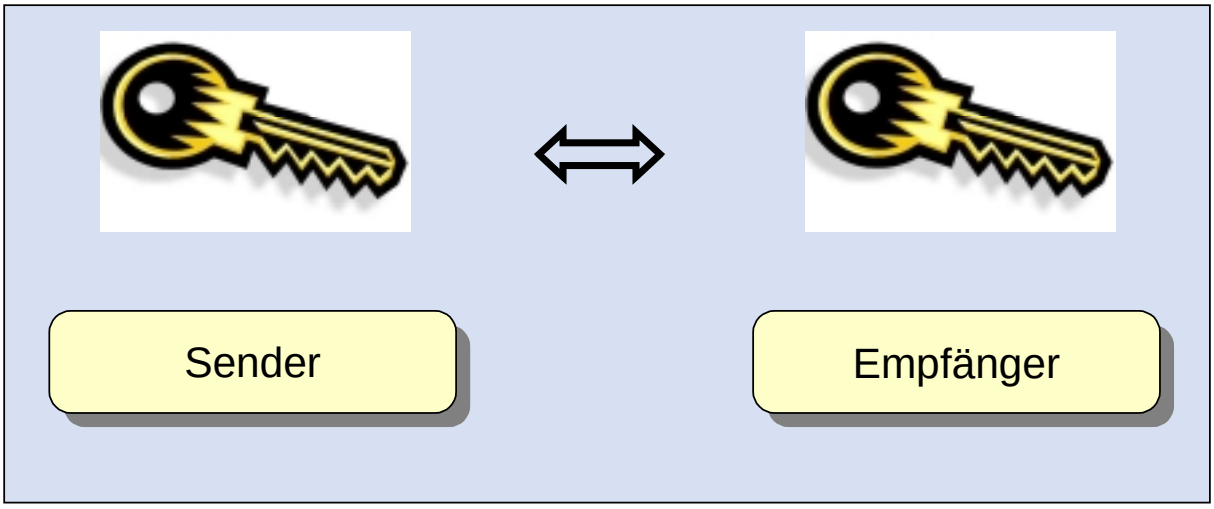

Abbildung 5-1: Symmetrische Verschlüsselung

Sowohl der Sender, als auch der Empfänger, benutzen den gleichen Schlüssel. Der Sender verschlüsselt mit Hilfe dieses Schlüssels seine Nachricht, und der Empfänger kann mit genau dem gleichen Schlüssel die Nachricht entschlüsseln. Dieses System ist solange vor Dritten sicher, solange diese den geheimen Schlüssel nicht kennen. Der Schwachpunkt ist jedoch die Kommunikation zwischen dem Sender und Empfänger, in der sich die beiden auf einen gemeinsamen Schlüssel einigen. Wird diese Kommunikation abgehört, so ist der Schlüssel bekannt und die nachfolgende verschlüsselte Kommunikation unsicher.

Dieser Schwachpunkt wird durch die **asymmetrische Verschlüsselung** bzw. ein hybrides Verschlüsselungsverfahren ausgeschaltet. Hier existieren sowohl bei dem

Sender als auch bei dem Empfänger zwei Schlüssel. Einer dieser beiden Schlüssel ist privat und einer öffentlich. Der Sender kodiert nun die Nachricht mit dem öffentlichen Schlüssel des Empfängers. Dieser Schlüssel kann jedoch nicht zur Entschlüsselung der Nachricht verwendet werden; hierzu wird stattdessen der private Schlüssel des Empfängers benötigt.

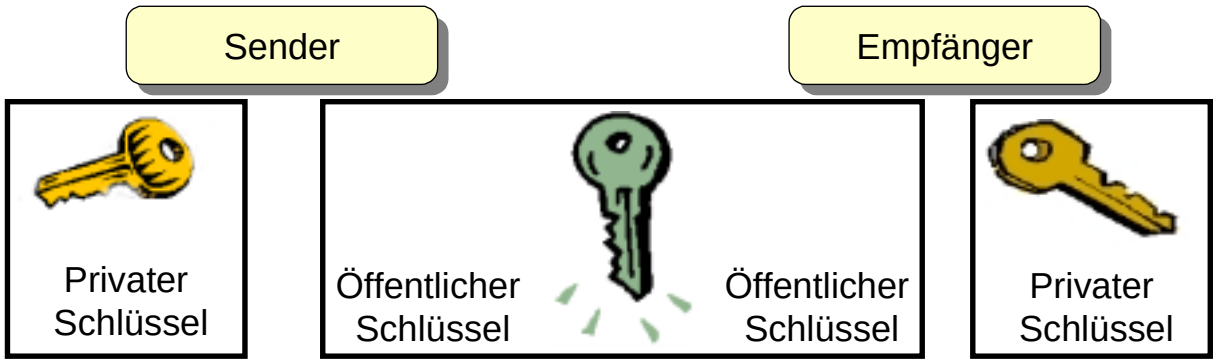

Abbildung 5-2:Asymmetrische Verschlüsselung

Durch dieses System wird kein geheimer Generalschlüssel mehr benötigt, sondern man kann sich darauf verlassen, dass jeder Teilnehmer seinen privaten Schlüssel möglichst geheim hält.

Die asymmetrischen Verschlüsselungsverfahren benötigen wesentlich mehr Rechenleistung als symmetrische Verfahren. Daher werden oft hybride Verfahren eingesetzt.

b) PGP (Pretty good Privacy)

Bei PGP (Pretty Good Privacy) handelt es sich um eine im Internet weit verbreitete Software, mit der man E-Mails verschlüsseln und digital signieren kann. Das Programm, das 1991 vom US-Amerikaner Phil Zimmermann entwickelt wurde, lässt sich auf allen gängigen Betriebssystemen einsetzen. Es basiert auf asymmetrischer Verschlüsselung, d.h. jeder Nutzer besitzt ein Paar aus einem öffentlichen Schlüssel, den er seinen Kommunikationspartnern zur Verfügung stellt, und einem privaten Schlüssel, den er geheim halten muss, damit nur er die Nachrichten an ihn entschlüsseln kann. Die Nachricht wird mit einem durch den RSA-Algorithmus (benannt nach den Entwicklern: Rivest, Shamir, Adleman) erzeugten Schlüssel unter Benutzung des IDEA-Algorithmus (International Data Encryption Algorithm (128-Bit)), verschlüsselt. Für Authentizitäts-Überprüfungen wird eine „Unterschrift" (Signatur) verwendet, die der Absender mit seinem privaten key erstellt. Wer die „Unterschrift" mit dem entsprechenden public key entschlüsselt, weiß dann, dass die Nachricht nur von dem bestimmten Absender kommen kann.

Die Verschlüsselung war so stark, dass nicht einmal die National Security Agent der USA den Code knacken konnte.

c) Firewall

Eine Firewall (Brandschutzmauer) ist ein Software Paket welches an Netzwerkübergangspunkten (z.B. Internet Gateway), Servern oder Desktop Systemen installiert wird. Es dient zur Durchsetzung einer Sicherheitspolitik, indem es alle ein- und ausgehenden Datenpakete untersucht, sie mit der Sicherheitspolitik vergleicht und eine Entscheidung trifft, ob diese durchgelassen oder abgeblockt werden. Es wird dafür gesorgt, dass jede Kommunikation zwischen zwei Netzen über die Firewall geführt werden muss. Auf dem Firewall sorgen Zugriffskontrolle und Audit (Überprüfen und testen der Firewall-Konfiguration) dafür, dass potentielle Angriffe schnellstmöglich erkannt werden.

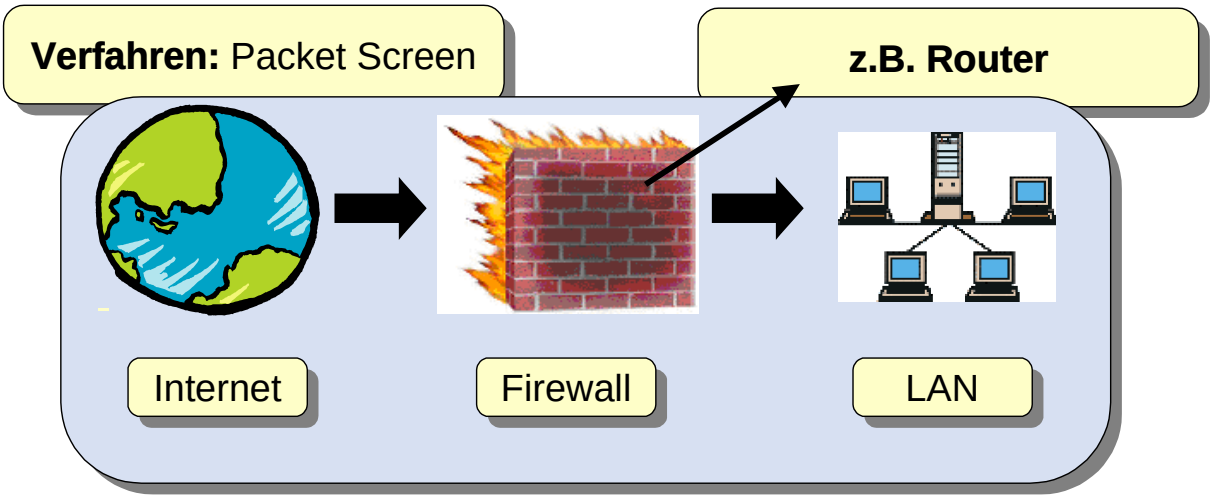

Abbildung 5-3: Aufbau Firewall

Eine häufig verwendete Möglichkeit zum Aufbau einer Firewall ist das sogenannte Packet Screen. Dabei wird zum Beispiel ein bestehender Router zwischen LAN und Internet so konfiguriert, dass er nur bestimmt Pakete durchlässt und andere abblockt.

Die Möglichkeit für den privaten Internet-Nutzer sich vor ungewollten Zugriffen zu schützen besteht in einer Firewall, die er durch entsprechende Software auf seinem Rechner installieren kann. Diese lässt sich zum Beispiel so konfigurieren, dass nur noch gewollte Dienste, wie FTP oder WWW und deren zugehörige Ports freigegeben werden. Bei anderen Fremdzugriffen gibt das Programm eine Warnmeldung aus.

5.1.2 Sicherheitslücken von Innen und Gegenmaßnahmen

Ein großes Problem, das heute einen immensen Schaden anrichtet ist die innere Sicherheit eines Netzwerkes. Hierzu gehören der Zugang und der Zugriff auf das Netzwerk. Ein großer Teil der ausgespähten Daten wird nicht über das Internet übertragen, sondern direkt von Personen innerhalb des Netzwerkes. Die Daten werden dann zum Beispiel über Disketten oder andere Medien „geraubt“. Um dieser und anderer interner Spionage zu begegnen, sind folgende Maßnahmen für z.B. Firmennetzwerke unverzichtbar:

1. Es ist zu prüfen wer **Zugang** zu kritischen Systemen haben soll, wer Verwaltung und Kontrolle der Zugangsmittel und -berechtigungen übernimmt. Auch physische Vorraussetzungen wie die Gebäudesicherheit usw. sollten geprüft werden.
2. Der **Zugriff** auf die Daten und Anwendungen der Computersysteme durch Benutzerverwaltung, Rechtevergabe, Beschränkung von Anwendungen und Diensten, sichere Benutzerauthentisierung, Passwort-Systeme usw. muss geregelt sein.
3. Auch intern besteht die Gefahr von z.B. **Viren oder Trojanern**. Wichtige IT-Systeme sollten daher durch zentrale und verteilte Virenscanner (Schutzprogramme) geschützt werden.
4. Der **Datentransfer** nach außen und unter Mitarbeiter sollte auf das nötigste Volumen reduziert sein.
5. **Ungeprüfte Datenträger** von außen dürfen keinesfalls benutzt werden. In vielen Betrieben ist eine Missachtung Kündigungsgrund.
6. Daten sollten regelmäßig auf Zweitmedien, sogenannten **Backup-Systemen**, gesichert werden. Wie dies geschieht zeigen die Methoden im folgendem Kapitel.

5.2 Datensicherung

5.2.1 Sicherungsmedien

Zur Datensicherung lassen sich unterschiedliche Medien, je nach Verwendungszweck und Datenvolumen verwenden. Die dabei gebräuchlichsten werden im Folgendem erläutert:

Die **Diskette** ist ein Speichermedium mit einem relativ kleinen Speichervolumen von nur 1,44MB. Sie besteht aus einer flexiblen Kunststoffscheibe auf der die Daten gespeichert werden. Zum Lesen ist ein Diskettenlaufwerk, auch „Floppy“ genannt notwendig. Disketten werden heute immer weniger benutzt, da kleine Datenmengen ohne großen Zeitaufwand im Internet verschickt werden können oder andere Speichermedien wie CD-ROMs für nur wenig mehr Geld einen immens größeres Speichervolumen besitzen. Populärer sind heute andere Arten von Disketten, wie z.B. ZIP-Laufwerke mit Speichervolumen von 100MB oder auch Wechselplatten, deren Speichervolumen schon an gängige Festplatten heranreicht.

Die **CD-ROM** (Compact Disc – Read Only Memory) die ursprünglich für den Musikmarkt von Philips entwickelt wurde basiert auf einen Laser, der digital abgespeicherte Daten optisch abtastet und sie somit auch nach längerer Zeit ohne Qualitätsverlust lesen kann (optisches Speichermedium). Im Vergleich zur Diskette ist das Speichervolumen mit durchschnittlich 682MB etwa 50fach höher. Es stehen heute verschiedene Arten der CDs für die Datensicherung zur Verfügung. Die populärsten sind die CD-R (für „recordable“) und CD-RW (für „rewriteable“). Beide Können mit CD-Brennern beschrieben werden, die CD-RW hat dabei den Vorteil das sie mehrfach beschrieben werden kann. Zum Lesen von CDs sind CD-ROM-Laufwerke, DVD-Laufwerke oder CD-Brenner notwendig. Viel diskutiert wird die Haltbarkeit von CD-ROMs. Einige Hersteller geben Ihren CDs bis zu 100 Jahren Haltbarkeit, realistischer scheinen jedoch Einschätzungen von Experten, das bei vielen CD-ROMs das Lesen der Daten schon nach 20 Jahren Problem bereitet.

Eine **Festplatte** besteht aus mehreren übereinander rotierenden Magnetplatten, welche in einem luftdicht verschlossenen Gehäuse montiert sind. Neuste Festplatten bestehen mitunter aus nur noch zwei Magnetplatten. Die Datentransferraten sind mindestens das zehnfache höher als bei Disketten, weil sie sich mit der zehnfachen Geschwindigkeit drehen je nach Typ zwischen 3500 und 7200 U/min. Der Vorteil einer Festplatte liegt in Ihrem großen Speichervolumen, bei heutigen Festplatten schon über 100Gigabyte. Als Nachteil kann gesehen werden, dass Festplatten fest in den Rechner eingebaut sind und somit nicht ein „mobiles“ Medium wie Disketten oder CD-ROMS sind. Neben dem Speichervolumen haben Festplatten den Vorteil hoher Geschwindigkeiten beim Datentransfer. Gerade beim Löschen und beschreiben großer Datenmengen ist dieses von Vorteil.

Streamer ist eine andere Bezeichnung für ein Magnet-Laufwerk. Der Ausdruck "Streamer" entstammt dem englischen Begriff "stream", der u.a. Strom bedeutet.

Gemeint ist damit der kontinuierliche Daten-Strom, der sequentiell auf das Band übertragen wird. Je nach Typ können auf diese Magnet-Bänder Datenmengen bis in den Terabyte-Bereich geschrieben werden. Sie sind für die Datensicherung von Firmennetzwerken u.a. von großer Bedeutung. Der Nachteil von Streamern liegt jedoch in der Schreibgeschwindigkeit, sodass es durchaus möglich ist, dass ein Backup mehrere Stunden oder Tage dauern kann. Auch die Haltbarkeit von magnetischen Bändern ist eher gering, da sich mit der Zeit die Magnetpartikel von selbst ausgleichen.

5.2.2 Daten- und Verfügbarkeitssysteme

Es lassen sich zwei Arten der Datensicherung unterscheiden. Bei den Datensystemen werden große Datenmengen durch ein Backup-System gesichert. Verfügbarkeitssysteme haben die Aufgabe Daten möglichst lange zur Verfügung zu stellen um bei einem Ausfall des Systems sofort weiterarbeiten zu können. Beispiele für diese beiden Varianten sind Roboter die Magnetbänder austauschen(Backup-System) und das RAID-System als Verfügbarkeitssystem.

Das **RAID**-System (**R**edundant **A**rray of **I**ndependent **D**isks) ist in der Lage, Daten redundant, also auf mehrere Festplatten gleichzeitig zu schreiben. Dazu sind je nach RAID-Level mehrere Festplatten gleicher Größe, besser noch gleichen Typs notwendig. Beim RAID-0-System werden die Daten auf zwei gleiche Festplatten abwechselnd geschrieben. Die 0 steht für keine „Redundanz“, also keine Sicherheit. Es ist lediglich eine Performance-Steigerung des Systems zu erreichen, z.B. für die Verarbeitung von digitalen Videodateien. In einem RAID-1-System, auch "Drive Duplexing" genannt, werden auf zwei Festplatten identische Daten gespeichert. Es ergibt sich damit eine Redundanz von 100 Prozent. Fällt eine der beiden Platten aus, so arbeitet das System mit der verbleibenden Platte ungestört weiter. Die hohe Ausfallsicherheit dieses Systems wird allerdings meist nur in relativ kleinen Servern eingesetzt, da bei RAID 1 die doppelte Platten-Kapazität benötigt wird, was sich bei großen Datenmengen schnell finanziell bemerkbar macht.

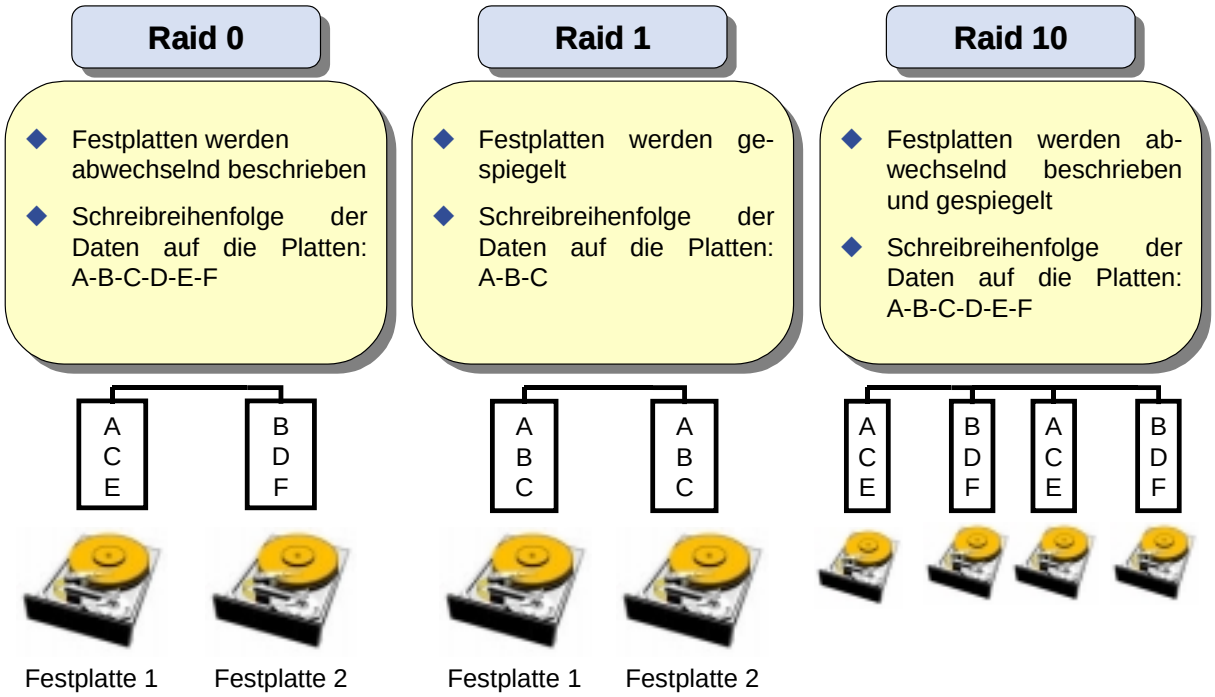

Abbildung 5-4: Raidsysteme

Ein weiteres, sehr gebräuchliches Backup-System ist RAID 10, bzw. RAID 0+1. Es handelt sich hier nicht um einen eigenen RAID-Level, sondern lediglich um die Kombination von RAID 1 mit RAID 0. Damit werden die Eigenschaften der beiden "Mutter-Levels" - Sicherheit und sequentielle (zusammenhängende) Performance vereinigt.
Bei RAID 10 bzw. RAID 0+1 werden vier Festplatten verwendet, denn dieses System verlangt nach zwei Paaren gespiegelter Arrays, die dann zu einem RAID-0-Array zusammengefasst werden. Insbesondere zur redundanten Speicherung von großen Dateien eignet sich RAID 10. Die Schreibzugriffe mit RAID 10 sind sehr schnell, da hierbei keine Parität berechnet werden muss. RAID 10 gilt übrigens auch als zusätzlich gestripte Version von RAID 1. Unterschiedliche Kombination von Raid-Systemen lassen weitere RAID-Level zu. So wären z.B. für einen Kombination von RIAD-0 und RAID-1 vier Festplatten notwendig.

Bei großen Datenmengen sorgen **Backup-Systeme** für die notwendige Datensicherheit. Hier werden die Daten nicht nur gespiegelt, wie es bei RAID der Fall ist, sondern es ist auch eine Dateiverwaltung möglich. Als Sicherungsmedien werden häufig Magnetbänder eingesetzt, da diese eine sehr hohe Speicherkapazität besitzen und günstiger als andere Medien sind. Die Daten werden zum Beispiel auf externe Kassettenbänder geschrieben und mit Hilfe eines Roboters zwischen Lagerplatz und den Laufwerken transportiert (Abbildung 5-5).

Abbildung 5-5: Magnetband Backup-System (Quelle: www.kes.info/)

Zur Speicherung gibt es neben den "klassischen" Magnetbandkassetten vom Typ IBM 3480/3490 (Kapazität ca. 200 - 800 MByte unkomprimiert) mittlerweile viele Medien wie beispielsweise DAT, Exabyte, Metrum-VHS, DLT, D1 und D2, deren Kapazitäten bereits im Bereich mehrerer bis vieler GByte pro Kassette liegen und die systembedingt unterschiedliche Leistung bieten.

Bei Backup-Systemen mit optischen Speichermedien wird die Aufgabe des Datenträgerwechsels von „Jukeboxen“ übernommen. Jukeboxen erlauben heute einen Zugriff auf nahezu unbegrenzte Datenmengen.

5.2.3 Sicherungsstrategien

Grundsätzlich wird zwischen drei Arten der Backup-Strategien unterschieden.

Volles Backup (full backup):

Hier werden alle Daten (oder bestimmte Datenpfade) eines Rechnersystems unabhängig von Alter einzelner Datenfiles gesichert.

Vorteil: Einfaches und schnelles Restaurieren ganzer Verzeichnisebenen oder eines ganzen Rechnerbestandes; Nachteil: Lange Backupzeiten.

Differentiell inkrementelles Backup (differentieller Backup):

Es werden alle Daten gesichert, die seit der letzten Datensicherung (gleich welcher Art) modifiziert oder neu angelegt wurden.

Vorteil: kurze Backupzeiten, wenig Backupvolumen, geringe Netz- und Rechnerlast; Nachteil: bei Wiederherstellen ganzer Verzeichnisebenen bzw. kompletter Rechnerdatenbestände müssen alle inkrementellen Backups seit dem letzten vollen bzw. differentiellen Backup eingelesen werden. Dies führt zu höherem administrativem und zeitlichem Aufwand.

Kumulativ inkrementelles Backup (inkrementeller Backup):

Es werden alle Daten gesichert, die seit der letzten vollen Datensicherung (Gesamtsicherung) modifiziert oder neu angelegt wurden.

Vorteil: Die Wiederherstellung ganzer Verzeichnisebenen bzw. kompletter Rechnerdatenbestände ist relativ einfach, da nur der jeweils aktuelle kumulativ inkrementelle Backup und der letzte Fullbackup zurückgespielt werden; Beim Einsatz kumulativ inkrementeller Backups kann man die Fullbackups in längeren Intervallen durchführen. Nachteil: Je länger der Zeitraum zwischen den Fullbackups wird, desto stärker wächst das Volumen der kumulativ inkrementellen Backups (im Vgl. zu den differentiell inkrementellen Backups).

Eine Mischung der drei Strategien (z.B. zweiwöchentliches Fullbackup, wöchentliches inkrementelles Backup, tägliches differentielles Backup) gewährleistet in der Regel eine ausgewogene und zuverlässige Datensicherung.

6 Zusammenfassung

Bei der Kommunikation zwischen Menschen hat die Informationsverbreitung heute eine entscheiden Rolle: Sie dient dem Transport der Daten und lässt eine besonders schnelle Kommunikation zu. Diese Kommunikation braucht Kommunikationsnetze, die durch Computernetzwerke realisiert werden. Der Aufbau eines solchen Netzwerkes kann zentral als Client-Server-Konzept oder dezentral Peer-to-Peer-Netzwerk gestaltet werden.

Wie im Straßenverkehr kann bei der Abwicklung des Datenverkehrs im Bereich der EDV zwischen Verkehrswegen und Verkehrsregeln unterschieden werden. Die physikalische Topologie ist mit den Verkehrswegen gleich zu setzten, die logische Topologie mit den Verkehrsregeln, den Zugriffsverfahren.

Als Übertragungsmedien können leitergebundene (z.B. Kupfer- oder Glasfaserleitungen) oder leiterungebundene Übertragungsmedien (z.B. Luft) dienen.

Um die Datenübertragung in der Informationstechnik darzustellen, wird das OSI-Referenz-Modell als Grundlage genutzt. Dieses ist in sieben Schichten aufgebaut, die bei der Datenübertragung eigenständige Funktionen haben.

Netzwerke auf lokaler Ebene werden als LAN bezeichnet. LANs begrenzen sich in der Regel auf einzelne Gebäude. Netzwerke über eine ganze Stadt werden als MAN bezeichnet. Netzwerke mit kontinentaler Ausdehnung werden WAN genannt. Das denkbar größte Netzwerk ist das Internet. Grundlage hierfür bilden die Hauptleitungen, (Backbones), Neutrale Austauschstellen und Router, über die der Datenverkehr läuft. Um Dateien zu übertragen werden Dienste wie das WWW zur Verfügung gestellt, welche über die TCP/IP Protokollfamilie ausgeführt werden. Zu dieser Protokollfamilie gehören beispielsweise http zum Übertragen von Internetseiten oder FTP zur Datenübertragung. Jeder Computer innerhalb des Internet ist durch seine IP-Adresse genau identifizierbar.

Durch eine globale Vernetzung von Computern und einer möglichen Nutzung durch Jedermann, birgt das Internet einige Sicherheitsgefahren. Empfangene Dateien können Viren, Trojaner oder Internetwürmer beinhalten. Gemeinsam ist ihnen, dass es ausführbare Programme sind die in erster Linie geschrieben wurden um Schaden anzurichten. Häufig sind solche Programme nur schwer erkennbar und die Verbreitung geschieht mit Unwissenheit des Benutzers. Der jährliche Schaden ist

daher immens. Aus diesem Grund sind Gegenmaßnahmen für Firmen und auch Privatleute von besonderer Bedeutung. Möglichkeiten zum Schutz bilden u.a. Virenscanner, restriktive Vergabe von Zugriffsrechten und auch das Vermeiden vom Speichern vertraulicher Daten (z.B. Passwörter) auf Festplatten.

Ein weiteres Problem ist das Sichern von Daten. Nach einem Datenverlust durch Systemabstürze, Viren, etc. ist es besonders für Firmen-LANs überlebenswichtig, die verlorenen Daten wiederherzustellen und den Verlust möglichst klein zu halten. Daher werden Backup- und Verfügbarkeitssysteme eingesetzt, die in festen Zeitintervallen, je nach Bedarf die Daten auf Sicherungsmedien, wie zum Beispiel Streamern speichern und ein Wiederherstellen des Systems vereinfachen, ohne großen Daten- und Zeitverlust.

7 Literatur

[1] Eckert, C.: IT-Sicherheit: Konzepte-Verfahren-Protokolle, Oldenburg 2001

[2] Wilde, E.: World Wide Web Springer Verlag. Berlin, 1999

[3] Shannon, C. E.; Weaver, W.: Mathematical Theory of Communication, University of Illinois Press, 1963

[4] Hafner, K.; Lyon, M.: Die Geschichte des Internet, 2. Auflage dpunkt.verlag. Heidelberg, 2000

[5] RRZN/Universität Hannover: Grundlagen Netzwerke, 4. Auflage Hannover 2001

[6] Hering, E., Gutekunst, J., Dyllong, U.: Handbuch der praktischen und technischen Informatik, 2. Auflage. Springer Verlag. Berlin, Heidelberg, u.a., 2000

[7] Tuepflis Global Village Library: **http://www.payer.de/cmc/cmcs01.htm** (29.01.02)

[8] Uniklinik Saarland: http://www.uniklinik-saarland.de/zik/hubedv.html 13.02.02

[9] Universitätsklinikum Aachen: http://www.klinikum.rwth-aachen.de/cbt/hypertext/asymmkey.html 18.02.02

[10] DFN-CERT "Zentrum für sichere Netzdienste" GmbH http://www.cert.dfn.de/team/ue/fw/workshop/node2.html 18.02.02

[11] Computer Graphics, TU Braunschweig: http://www.cg.cs.tu-bs.de/goepffarth#PGP (19.02.02)

[12] Universität der Bundeswehr München: http://www.unibw-muenchen.de/campus/RZ/Server/backupsrv/lexikon.html (19.02.02)

[13] Uni Münster: Rechnernetze und Internet technische Grundlagen http://www.uni-muenster.de/ZIV/Lehre/2000-4/RechnernetzeTechnischeGrundlagen/v02.pdf 24.04.02

[14] media connect service 24, http://www.internet-manual.de/technik.htm 24.04.02

[15] Uni Düsseldorf: Kursunterlagen Grundlagen Netzwerke, http://www-public.rz.uni-duesseldorf.de/~hoffv/netzwerk.html 24.04.02