

# Small LAN

kleine Netzwerke



Gerd Gerhardus

1.	Vor- und Nachteile .....	5
1.1.	Die Vorteile.....	5
1.1.1.	Zentrale Datenablage .....	5
1.1.2.	Benutzerverwaltung.....	5
1.1.3.	Gemeinsame Nutzung von Geräten .....	5
1.1.4.	Redundante Systeme .....	5
1.1.5.	Gemeinsamer Internetzugang via Router .....	6
1.1.6.	Zentrale Kommunikationssysteme .....	6
1.2.	Nachteile .....	6
1.2.1.	Chaotische Datenstrukturen .....	6
1.2.2.	Anfälligkeit der gesamten EDV bei schlechter Einrichtung / Wartung.....	6
2.	Grundlagen .....	7
2.1.	So funktioniert TCP/IP .....	7
2.1.1.	Protokollarchitektur.....	8
2.1.2.	Die Kapselung von Daten .....	9
2.1.3.	IP: Internet Protocol.....	10
3.	Netzwerkplanung.....	11
3.1.	Grundplanung .....	11
3.2.	Kabelsystem .....	11
3.2.1.	Kleine Kabelkunde.....	12
3.3.	Hardwareplanung.....	12
3.3.1.	Bestandsaufnahme .....	12
3.3.2.	Teilleiste .....	13
3.4.	Netzwerke ausfallsicher konzipieren .....	15
3.4.1.	Voraussetzung: Management.....	16
3.4.2.	Grundregeln für das Netzdesign.....	17
3.4.3.	Einfache Konfiguration wichtig .....	18
3.5.	Betriebssysteme .....	19
3.6.	Datensicherung.....	19
3.7.	Netzwerkschutz .....	19
3.7.1.	Die Firewall .....	20
3.7.2.	Antivirenprogramme.....	21
4.	Netzwerkkommunikation.....	21
4.1.	Protokolle .....	21
4.1.1.	TCP / IP .....	22
4.2.	Windowsprotokolle .....	22
5.	Anhang .....	24
5.1.	Normen - Grenzwerte für Cat5, Cat6 und Cat7 .....	24
6.	Literaturhinweise.....	25
6.1.	Internet & Netzwerk .....	25
6.2.	Allgemeines .....	25

Die Informationen in diesem Produkt werden ohne Rücksicht auf einen eventuellen Patentschutz veröffentlicht. Warennamen werden ohne Gewährleistung der freien Verwendbarkeit benutzt. Bei der Zusammenstellung von Texten und Abbildungen wurde mit größter Sorgfalt vorgegangen. Trotzdem können Fehler nicht vollständig ausgeschlossen werden. Herausgeber und Autor können für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen. Für Verbesserungsvorschläge und Hinweise auf Fehler sind Herausgeber und Autor dankbar.

Bitte senden Sie Ihre Anregungen an

Cyber Engineering

Gerd Gerhardus

Friedrichstrasse 2

42781 Haan /Germany

Mail@Cyber-Engineering.de

Alle Rechte vorbehalten, auch die der fototechnischen Wiedergabe und der Speicherung in elektronischen Medien. Die gewerbliche Nutzung der in diesem Produkt gezeigten Modelle und Arbeiten ist nicht zulässig.

Die Verwendung von Material aus diesem Produkt jeglicher Art sind nur mit schriftlicher Genehmigung des Autors oder Herausgebers gestattet.

Fast alle Hardware- und Softwarebezeichnungen, die in diesem Produkt erwähnt werden, sind gleichzeitig auch eingetragene Warenzeichen oder sollten als solche betrachtet werden.

© Gerd Gerhardus

© 2009 Cyber Engineering Gerd Gerhardus, Friedrichstrasse 2, 42781 Haan / Germany

Alle Rechte vorbehalten

Printed in Germany

Netzwerke sind heute aus dem Arbeitsalltag nicht mehr wegzudenken. In jeder Firma spielt das Netzwerk eine zentrale Rolle, meist erst bemerkt, wenn „gar nichts mehr geht“. Es geht bei weitem nicht mehr um die einfache Verbindung zwischen den einzelnen Maschinen. Gefragt sind Lösungen, die auf der einen Seite Ressourcen<sup>1</sup> für Gruppen oder ganze Unternehmen bereitstellen – beispielsweise Drucker, Faxprogramme, Terminalsysteme, Warenwirtschaftslösungen aber auch der Internetzugang – auf der anderen Seite eine zentrale Plattform für die unternehmensinterne Kommunikation bieten sollen. Hier geht es um einfache Wege, Konferenzen zu Terminieren, Wissensdatenbanken bereitzustellen, ...

Ich möchte dem Leser möglichst einfach skizzieren, welchen Prinzipien die aktuellen Netzwerke folgen und welche Möglichkeiten – aber auch Gefahren und Probleme – für Anwender aus einem Netzwerk erwachsen.

---

<sup>1</sup>Im EDV Sprachgebrauch versteht man unter Ressourcen Geräte und Programme

## 1. Vor- und Nachteile

Wie fast alles im Leben gibt es auch bei Netzwerken zwei Seiten der Medaille...

### 1.1. Die Vorteile

#### 1.1.1. Zentrale Datenablage

Der wohl wichtigste Punkt ist die zentrale Speicherung von Daten auf dem Server. Hieraus ergibt sich die Möglichkeit, daß alle Benutzer auf alle Daten – sofern sie darauf Zugriffsrechte haben – zugreifen können. Ein weiterer wichtiger Aspekt ist die zentrale Datensicherung.

#### 1.1.2. Benutzerverwaltung

Alle modernen Server-Betriebssysteme haben eine Benutzerverwaltung. Diese regelt zum einen, wer überhaupt Zugriff auf den Server hat, zum anderen, was der Berechtigte denn nun wirklich darf. Zur leichten – und damit kostengünstigeren – Administration läuft die Benutzerverwaltung auch in Mehr-Server-Umgebungen zentral.

#### 1.1.3. Gemeinsame Nutzung von Geräten

Dieser Punkt ist für Unternehmen entscheidend. Hier werden erhebliche finanzielle Mittel eingespart, indem nicht jeder Mitarbeiter einen kleinen Drucker am Platz hat, sondern große Drucker oder Kopiergeräte für ganze Abteilungen genutzt werden. Weiterhin kann so auch ein schneller Internetzugang für das ganze Unternehmen kostengünstig realisiert werden.

#### 1.1.4. Redundante Systeme

Schon sind wie bei der Ausfallsicherheit des Netzwerkes. Es wäre unbezahlbar, wenn für jeden Mitarbeiter zwei PCs parat stehen müßten, auf denen permanent alle Daten liegen. Bei Servern sind die Kosten pro Mitarbeiter überschaubar. Hier stellt man mehrere gleiche Maschinen nebeneinander, die alle die gleiche Arbeit machen. Zum einen läuft das Netzwerk schneller, zum anderen fällt es beim Ausfall eines Servers nicht aus. Ebenso kann bei Problemen mit einem Drucker auf ein anderes Gerät ausgewichen werden.

### 1.1.5. Gemeinsamer Internetzugang via Router

Es ist nicht nur die preiswertere Variante, einen Internetzugang gemeinsam zu nutzen; hier lohnt sich auch die Investition in Sicherheitsmechanismen wie Router und Firewall.

### 1.1.6. Zentrale Kommunikationssysteme

Eine große Arbeitserleichterung sind zentrale Kommunikationslösungen wie EMail, Faxsysteme und Terminkalender. So ist es unproblematisch, einen Termin für die zwanzig Teilnehmer einer Konferenz zu finden; die Software sucht automatisch nach dem nächsten Termin, an dem alle Zeit haben.

## 1.2. Nachteile

Auch die Nachteile sollen hier kurz aufgezeigt werden.

### 1.2.1. Chaotische Datenstrukturen

Wir stellen häufig bei Neukunden eine sehr chaotische Datenstruktur fest. Dies führt dazu, daß zum einen Dateien etliche Male in verschiedenen Versionen an verschiedenen Orten gespeichert sind, zum anderen findet keiner mehr die aktuellen Dateien. Wie im kleinen, muß auch bei großen Datenmengen sehr auf eine einheitliche Struktur geachtet werden, die auch von jedem eingehalten werden muß.

### 1.2.2. Anfälligkeit der gesamten EDV bei schlechter Einrichtung / Wartung

Da das Netzwerk ein zentrales Werkzeug für das gesamte Unternehmen darstellt, hat ein Totausfall fatale Folgen. Bei schlecht geplanten, mangelhaft installierten oder unzureichend gewarteten Netzwerken können häufig kleine Fehler das gesamte Netzwerk zum Stillstand bringen. Gleiches gilt für lieblos eingerichtete Firewalls. In solchen Fällen breiten sich Viren sofort im ganzen Netzwerk aus und bringen alle Maschinen zum Stillstand.

## 2. Grundlagen

### 2.1. So funktioniert TCP/IP

Die Grundlage des Netzwerkes und des Internets ist TCP/IP, das eine weltweite Kommunikation zwischen unterschiedlichsten Systemen ermöglicht. Ich erläutere den Aufbau der Protokollsuite und gebe Ihnen einen Einblick in das Protokoll IPv6.

Die Protokollfamilie TCP/IP wurde erstmalig Mitte der 70er Jahre entwickelt, als bei der amerikanischen Defense Advanced<sup>1</sup> Research Agency (DARPA) das Interesse an einem Paketvermittlungsnetz aufkam, das die Kommunikation zwischen unterschiedlichen Computersystemen an Forschungseinrichtungen erleichtern würde. TCP/IP schafft ein heterogenes Netzwerk mit offenen Protokollen, die unabhängig von unterschiedlichen Betriebssystemen und Hardware-Architekturen sind. Ob Heim-PC, Großrechner oder Pocket-PC - über die Internet-Protokolle können alle Rechner miteinander kommunizieren.

Die Protokolle sind für jedermann frei verfügbar und werden als offen betrachtet. Jeder Anwender kann sie lizenzfrei für eigene Zwecke nutzen und eigene Applikationen und Dienste darauf aufsetzen. Dabei steht TCP/IP für eine ganze Reihe von Protokollen, der so genannten "Internet Protocol Suite". Die beiden wichtigsten Typen TCP und IP sind zum Synonym für diese Familie geworden.

Auf Grund des einheitlichen Adressierungsschemas kann jeder Rechner in einem TCP/IP-Netz jeden beliebigen anderen Rechner eindeutig identifizieren. Standardisierte Protokolle in den höheren Schichten stellen dem Benutzer einheitlich verfügbare Dienste zur Verfügung. Als TCP/IP Ende der 70er Jahre dem BSD-Unix<sup>2</sup> beigefügt wurde, entwickelte sich daraus die Grundlage, auf der das Internet basiert.

---

<sup>1</sup> <http://www.darpa.mil/>

<sup>2</sup> <http://www.bsd.org/>

## 2.1.1. Protokollarchitektur

Es gibt keine generelle Übereinstimmung darüber, wie TCP/IP in einem Schichtenmodell beschrieben werden soll. Das OSI-Modell<sup>1</sup> ist zwar recht nützlich, aber größtenteils sehr akademisch. Um den Aufbau von TCP/IP zu verstehen, benötigt man ein Modell, das näher an die Struktur der Protokolle angelehnt ist.

Das amerikanische Verteidigungsministerium (DoD - Department of Defense<sup>2</sup>) hat ein 4-Schichten-Netzwerkmodell ausgearbeitet. Jede Schicht besteht aus einer Anzahl von Protokollen, die gemeinsam die TCP/IP-Protokollfamilie bilden. Die Spezifikationen für jedes Protokoll wurden jeweils in einem oder mehreren RFCs<sup>3</sup> festgelegt.



Die Daten werden wie im OSI-Modell beim Versenden im Stack nach unten gereicht; beim Empfang von Daten aus dem Netz führt der Weg durch den Stack nach oben. Jede Schicht fügt dabei ihre Kontrollinformationen hinzu, um eine korrekte Übertragung der Daten sicherzustellen. Diese Informationen nennt man Header, da diese den eigentlichen Daten vorangestellt werden.

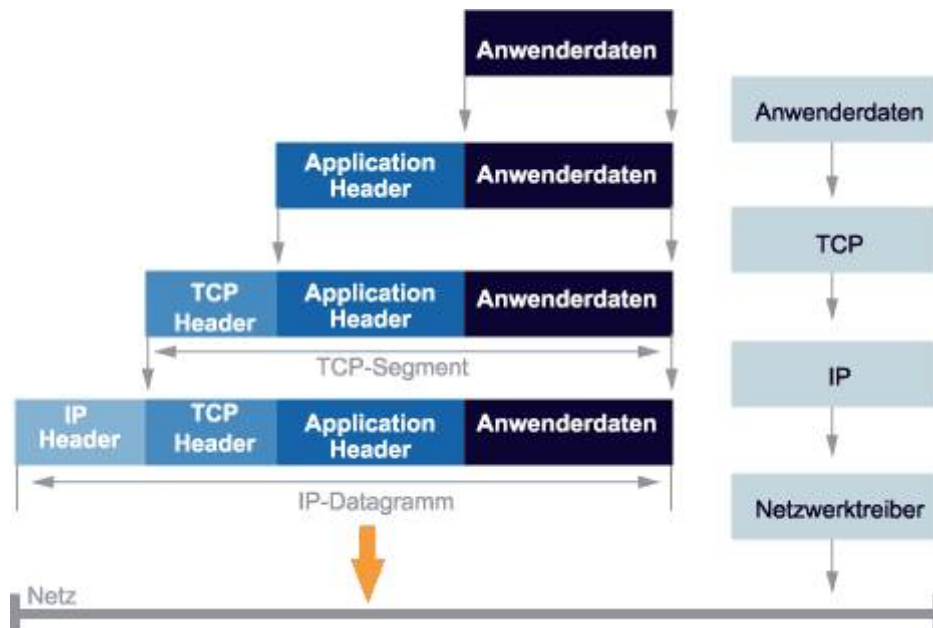
<sup>1</sup> OSI Open Systems Interconnect. Ein ISO-Standard für weltweite Kommunikation, der ein Rahmenmodell für die Implementierung von Protokollen in sieben Schichten definiert.

<sup>2</sup> <http://www.defenselink.mil/>

<sup>3</sup> RFC Request for Comments: Sammlung von Empfehlungen, Artikeln und Standards, in denen netzrelevante Konventionen und allgemeine Informationen zum Internet festgehalten sind.

## 2.1.2. Die Kapselung von Daten

Das Hinzufügen von Kontrollinformationen nennt man Encapsulation (Kapselung). Beim Empfangen von Daten werden die Schritte der Kapselung wieder rückgängig gemacht. Jede Schicht entfernt ihren Header und reicht die restlichen Daten an die darüber liegende Schicht weiter.








Kapselung: Zahlreiche Header vergrößern die Datenmenge bei TCP/IP.

Jede dieser Schichten verfügt über eine eigene, unabhängige Datenstruktur. In der Praxis sind aber die einzelnen Schichten so gestaltet, daß sie zu den Strukturen der benachbarten Schichten kompatibel sind. Dies dient der effizienteren Datenübertragung.

Bei der Übertragung von geringen Datenmengen kann es allerdings passieren, daß durch die Kapselung mehr Protokolldaten als Nutzdaten übertragen werden. In diesem Fall empfiehlt sich beispielsweise der Einsatz des User Datagram Protocols (UDP), welches über nur minimale Protokollmechanismen zur Datenübertragung verfügt.

### 2.1.3. IP: Internet Protocol

Das Internet Protocol (IP) ist die Grundlage der Protokollfamilie TCP/IP und für die Weiterleitung der Daten zuständig. Generell hat es die Aufgabe, die Datenübertragung zwischen Netzwerken sicherzustellen. Dazu muß das Protokoll diverse Aufgaben übernehmen und diese als Dienst den höheren Schichten zur Verfügung stellen. Zu den Aufgaben des IP zählen:

-  Datenpaketdienst
-  Fragmentierung von Datenpaketen
-  Wahl der Übertragungsparameter
-  Adreßfunktion
-  Routing zwischen Netzwerken

Die Hauptaufgabe des IP ist die Ermittlung und Realisierung des optimalen Weges zwischen Sender und Empfänger für jedes Datenpaket. Verbindungsaufbau und Verbindungsabbau fallen nicht in den Zuständigkeitsbereich dieses Protokolls.

Das Internet Protocol stellt keine gesicherte Verbindung zur Verfügung und kann keine verlorenen Datenpakete erneut übertragen. Jedes IP-Datenpaket wird als unabhängiges Paket (Datagramm) durch das Netzwerk an den Empfänger übermittelt. Für die Netzwerktypen sind unterschiedliche Datenpaketlängen festgelegt. Die Größe eines Datenpakets hängt von mehreren Faktoren ab, wie Hardware- und Software-Beschränkungen.

Ist ein Datenpaket wegen seiner Überlänge nicht als eine Einheit übertragbar, so muß es in kleinere Fragmente zerlegt werden. Die Pakete werden zwar in der richtigen Reihenfolge gesendet, kommen aber nicht notwendigerweise in derselben dort an. Da die Einzelpakete verschiedene Wege gehen können, sind zusätzliche Informationen erforderlich. Diese erlauben, den Zustand des ursprünglichen Datenpakets zu rekonstruieren. Jedes Datenpaket erhält daher bei der Übertragung einen IP-Header vorangestellt.

### 3. Netzwerkplanung

Um im späteren Betrieb mit möglichst wenig Fehlern kämpfen zu müssen, ist eine vorausschauende Planung sehr wichtig. Im Vordergrund steht immer der Sinn und Zweck des Netzwerkes, in der Regel ein bestimmtes Warenwirtschaftssystem. Die Probleme stecken im Detail, so daß jede Komponente genau bedacht werden sollte.

In die Netzwerkplanung fließen weitere Eckpunkte in Form von Vorgaben des Kunden ein, die teilweise nicht direkt mit der technischen Lösung zusammenhängen. Beispielsweise steht der optische Aspekt in Räumen mit Kundenverkehr im Vordergrund. Hier soll die Technik möglichst „unsichtbar“ sein. In anderen Fällen gehört es zum Image, die Technik zu zeigen: Ein Glasschrank mit Server und Telefonanlage steht im Flur. Oder der Server soll aus Sicherheitsgründen – Gefahr von Diebstahl der gesamten Maschine inklusive Daten – im Keller oder einer benachbarten Wohnung stehen.

#### 3.1. Grundplanung

Zunächst plane ich anhand von Grundriß oder Skizzen die Lage der Kabel. In dieser Phase wird lediglich zwischen Netzkabeln (die auch für die Telephonie zum Einsatz kommen) und Lichtleiterkabel differenziert. Dabei werden für die aktuellen Arbeitsplätze sowohl Netzwerk- als auch Telefonkabel berücksichtigt, ebenso die theoretisch maximale Arbeitsplatzzahl der Räume.

Daraus ergibt sich eine Teileliste der Verkabelung. Die wichtigsten Komponenten sind

-  Unterputzkabel
-  Kabelkanäle
-  Patchpanels
-  Dosen

#### 3.2. Kabelsystem

Die richtige Kabelwahl ist, solange man kein WLAN aufbauen möchte, das A und O in einem schnellen und Datenverlustfreien Netzwerk. Es gibt die unterschiedlichsten Kabelsorten für die jeweiligen Anwendungsgebiete. Faustregel ist: „Immer eine Nummer besser als benötigt, und nur von hoher Qualität!“ Denn: Die Kosten für die Kabel sind verschwindend gering im Vergleich zu den Kosten für den Arbeitsaufwand von Handwerkern, die entweder Kabel unter Putz oder in Kanälen verlegen und dann eine Renovierung durchführen müssen.

### 3.2.1. Kleine Kabelkunde

Netzwerkkabel werden meist als *Patchkabel* bezeichnet. Diese Kabel haben auf beiden Seiten einen *Westernstecker*, der entweder direkt in den Computer, die Dose in der Wand, ins *Patch-Panel*<sup>1</sup> oder ins Telefon gesteckt werden. Es ist also das Kabelstück, welches der Anwender auch sieht.

Die Güte eines Kabels wird häufig als *CAT5*, *CAT6* oder *CAT7* bezeichnet. Je höher die Zahl hinter dem „CAT“, desto schneller können auf dieser Leitung Daten übertragen werden. Der Anhang enthält eine Tabelle mit den entsprechenden Grenzwerten.

Um Störungen durch und auf das Kabel zu vermeiden, sind die Kabel geschirmt. Die gängigen Güten der Abschirmung sind *UTP*<sup>2</sup>, *S/UTP*<sup>3</sup> und *S/STP*<sup>4</sup>. Störungen treten beispielsweise durch schlecht abgeschirmten Kühlschränke, Mobiltelefone oder Aktivboxen auf, aber auch durch die Computer und Monitore selber.

## 3.3. Hardwareplanung

Ist die Grundplanung abgeschlossen, kommt der spannende Teil der Hardwareplanung. Der einfachste Fall ist eine komplette Neuplanung eines Netzwerks, denn ich muß keine Rücksicht auf vorhandene Hardware und eventuell auftretende Kompatibilitätsprobleme nehmen. Leider kommt das selten vor.

### 3.3.1. Bestandsaufnahme

Bei Erweiterungen, Umbauten oder Umzügen wird die vorhandene Hardware – soweit sinnvoll – weiter verwendet. Diese muß in einer Liste erfaßt und teilweise mit Verbesserungsvorschlägen versehen werden

---

<sup>1</sup>Das Patch-Panel ist eine Dosenleiste. Hier kommen etliche Netzwerkkabel aus der Wand und enden in den Dosen, in die dann wieder die Patchkabel gesteckt werden können.

<sup>2</sup>Unshielded Twisted Pair, ungeschirmtes 100 OHM Datenkabel, in USA Standard, sehr störanfällig

<sup>3</sup>Screened Unshielded Twisted Pair, geflechtgeschirmtes, paarverseiltes Datenkabel

<sup>4</sup>Screened Twisted Pair, geflecht- und foliengeschirmtes, paarverseiltes Datenkabel

### 3.3.2. Teileliste

Vom Bestand und der geplanten Verkabelung ausgehend wird nun eine Teileliste erstellt. Ich stelle hier die am häufigsten benutzten Hardwarekomponenten vor.

#### 3.3.2.1. Netzwerkkarte

Die Netzwerkkarte ist Bestandteil eines Computers und macht diesen erst *netzwerkfähig*. Früher als extra Karte zum Einbau geliefert, ist sie mittlerweile auf den meisten Hauptplatinen der Rechner fest integriert, bei Notebooks gehört sie zur Grundausstattung. Es gibt etliche verschiedene Modelle im Handel, die sich teilweise durch entscheidende Feinheiten unterscheiden. Die wichtigste Kennzahl für den Anwender ist der maximale Datendurchsatz. Hier gibt es drei Ausführungen: 10, 100 oder 1000 Mbit/s<sup>1</sup>.

#### 3.3.2.2. Hub

Ein Hub dient als „Mehrfachstecker“ im Netzwerk. Sollen also drei Geräte miteinander verbunden werden, so führt von jedem Gerät ein Patchkabel zum Hub. Dieser ist dann der zentrale Verteilerknoten (man spricht auch von einer *sternförmigen Netzwerktopologie*). Der Hub ist normaler Weise in der Lage, an jedem Ausgang die Geschwindigkeit des Endgerätes zu erkennen (10, 100 oder mehr MBit/s) und das Gerät in der entsprechenden Geschwindigkeit zu versorgen. Sollen also Daten von einem Rechner mit einer 100 MBit/s Karte zu einem Rechner mit einer 10 MBit/s Karte übertragen werden, so werden die Daten nur mit 10 MBit/s übertragen, da der sendende Rechner durch den Hub gebremst wird, weil dieser die Daten nicht schneller los wird.

#### 3.3.2.3. Switch

Ein Switch hat die gleiche Funktion wie ein Hub: Es verteilt den Datenverkehr im Netzwerk. Allerdings ist der Switch etwas „intelligenter“ als der Hub. Während der Hub alle Daten, die er empfängt, auf alle Ausgänge weiterleitet, erkennt der Switch, an welchem Ausgang welches Gerät angeschlossen ist. Er leitet dann die Daten nur an den Empfänger weiter und verursacht auf den anderen Leitungen keinen unnötigen Datenverkehr.

---

<sup>1</sup>1 MBit/s bedeutet, daß 1 Millionen Bit pro Sekunde (theoretisch) übertragen werden können. Dieser Wert entspricht 125 KB/s; somit könnte eine Datei mit 1 MB Größe in 8 Sekunden übertragen werden. Dieser Wert wird natürlich nie erreicht, denn die Daten werden in Paketen mit Zusatzinformationen übertragen, die übertragenden Geräte müssen sich ebenfalls „unterhalten“, ...

Deshalb sind Netzwerke, in denen ausschließlich Switches zum Einsatz kommen, auch bedeutend schneller. Einen Geschwindigkeitsunterschied bemerkt man bereits ab vier PCs.

Wie bei Hubs ist es auch bei Switches möglich, mehrere solche Geräte miteinander zu verbinden. Eine Beispielanwendung wäre ein Switch am Server, von dem aus Kabel in jeden Raum laufen. Daran hängt jeweils wieder ein Switch, an dem alle PCs des Raumes angeschlossen sind. (Diese Netzwerkrealisierung wäre nicht besonders glücklich, dafür aber mit sehr wenigen Kabeln zu realisieren.)

#### 3.3.2.4. Router

Ein Router ist ein Gerät, daß zwei verschiedene Netzwerke miteinander verbindet. Die Funktion wird als *Gateway*<sup>1</sup> bezeichnet. Typischer Anwendungsfall ist der Übergang zwischen verschiedenen logisch oder physikalisch getrennten Unternetzen in Unternehmen oder der Zugang zum Internet.

Neue Router sind Multifunktionsgeräte. Sie beinhalten neben der reinen Gateway-Funktion auch einen Switch, eine Firewall sowie etliche Konfigurationsmöglichkeiten für den Internetzugang über verschiedene Provider<sup>2</sup>.

---

<sup>1</sup>Als Gateway (dt. Eingang, Übergang) bezeichnet man eine Schnittstelle zwischen zwei grundsätzlich verschiedenen Netzwerksystemen

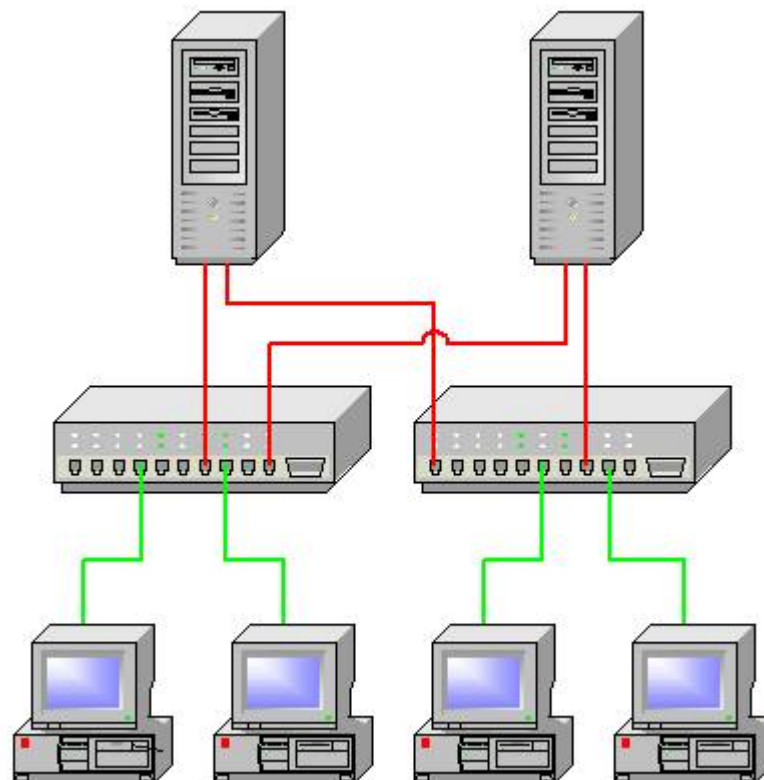
<sup>2</sup>Ein Provider (dt. Anbieter) vermarktet Zugänge zum Internet.

### 3.4. Netzwerke ausfallsicher konzipieren

Für die Ausfallsicherheit der Netzwerkinfrastruktur spielt das Design eine entscheidende Rolle. Neben teuren Hochverfügbarkeitslösungen gibt es auch Konzepte, die bereits für wenig Geld einen guten Schutz bieten.

Zuverlässige Netzwerkverbindungen sind für Unternehmen aller Größenordnungen sehr wichtig. Sie stellen sicher, daß der Zugriff auf die Geschäftsdaten immer möglich ist - egal ob diese auf dem Server, dem Storage-System oder den Mitarbeiter-PCs liegen.

Spielt Geld nur eine untergeordnete Rolle, dann läßt sich eine hohe Verfügbarkeit dadurch erreichen, daß man alle Netzwerk-Komponenten mindestens doppelt ausgelegt. Dies bietet zudem den Vorteil, daß sich Wartungsarbeiten an Switches und Routern vornehmen lassen, ohne den Netzbetrieb zu unterbrechen.



Doppelt hält besser: Wer die Kosten nicht scheut, kann sich durch eine doppelte Auslegung der Netzwerkkomponenten vor Hardware-Ausfällen schützen.

Um sich darüber hinaus vor Katastrophen wie Bränden, Erdbeben oder Flugzeugabstürzen zu schützen, unterhalten die meisten Großunternehmen geografisch getrennte Ausweichrechenzentren. Für kleinere und mittelständische Unternehmen kommen solche IT-Infrastrukturen aber aufgrund der damit verbundenen hohen Kosten meist von vornherein nicht in Frage.

Ich beschäftige mich deshalb in diesem Beitrag mit Technologien und Netzwerk-Designs, die bereits zu vergleichsweise niedrigen Kosten ein hohes Maß an Ausfallsicherheit bieten.

### 3.4.1. Voraussetzung: Management

Für den Aufbau von lokalen Netzen kommen heute aufgrund der stark gesunkenen Preise fast nur noch Switches zum Einsatz. Sie ermöglichen im Vergleich zu Hubs einen höheren Gesamtdurchsatz im Netzwerk, da sie die Daten vom Sender zum Empfänger über eine "geschwitchte" Verbindung direkt übertragen. Hubs dagegen sind ein Shared-Medium-Device, das die zu übertragenden Pakete an alle angeschlossenen Devices weitergibt.

Um eine redundante Switching-Infrastruktur aufzubauen, reichen die inzwischen sehr preisgünstigen unmanaged Switches nicht aus. Sie bieten zwar Funktionen wie automatische Geschwindigkeitserkennung oder ein selbstständiges Umschalten zwischen MDI- und MDI-X-Modus für Verbindungen zu anderen Switches. Entsprechende Fast-Ethernet-Geräte mit 8 Ports sind schon für unter 40 Euro zu haben, 24-Port-Switches für etwa 100 Euro. Derartige Switches lassen sich aber nicht für redundante Netzwerkverbindungen konfigurieren.

Die notwendigen Funktionen liefern erst die teureren managed Switches. Für redundante Topologien unterstützen sie auf Layer 2 das Spanning Tree Protocol (STP, IEEE<sup>1</sup> 802.1d) und dessen Nachfolger Rapid STP (RSTP, 802.1w) sowie Multiple Spanning Tree (802.1s) und das Link Aggregation Protocol (802.3ad). Diese Geräte bieten zudem meist SNMP<sup>2</sup>- und RMON<sup>3</sup>-Support, was die Verwaltung aus der Ferne ermöglicht. Für entsprechende managed Fast-Ethernet-Switches mit 24 Ports wandern allerdings ab 350 Euro aufwärts über den Ladentisch.

### 3.4.2. Grundregeln für das Netzdesign

Eine wichtige Grundregel des Netzdesigns besagt, daß es so einfach wie möglich gehalten werden sollte. Denn sobald ein Netz wächst, steigt zwangsläufig dessen Komplexität. Wurde bereits die Grundstruktur zu kompliziert angelegt, entwickelt sich das Ganze schnell zu einem unübersichtlichen und chaotischen Gebilde. Diese Regel erweist sich auch hinsichtlich der Verfügbarkeit als wichtig: Ein einfach strukturiertes, übersichtliches Netz läßt sich bei Problemen wesentlich schneller reparieren als ein undurchschaubares Netzwerkdickicht.

Generell gilt es zu beachten, daß auch eine redundante Auslegung aller wichtigen Hardware-Komponenten nur einen Teil der Ausfallursachen abdeckt. Häufig liegt der Grund für Netzwerkausfälle nicht in der Hardware begründet, sondern bei einer fehlerhaften Software. Auch in redundant ausgelegten Netzen kann durch Software-Fehler die gesamte Infrastruktur ausfallen, weil Switches oder Router vom gleichen Typ in der Regel dieselben Images verwenden. Um derartige Probleme so weit wie möglich zu vermeiden, sollten Administratoren nur die praxiserprobten Standardfunktionen der Switches einsetzen.

---

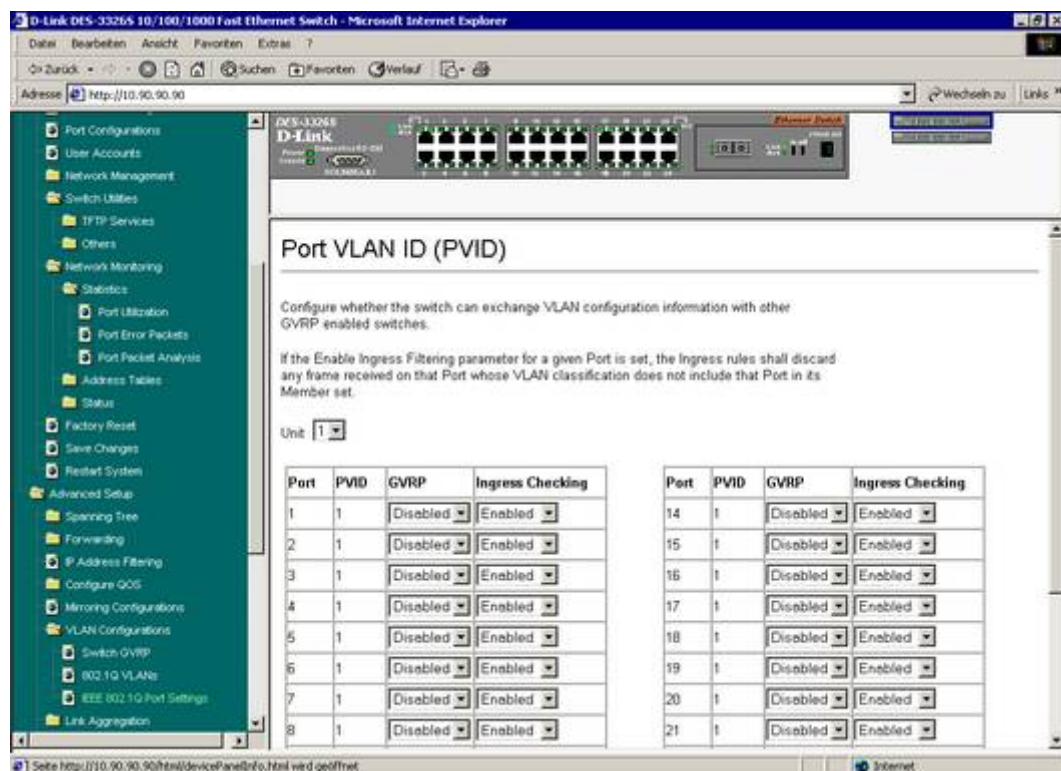
<sup>1</sup> IEEE Institute of Electrical and Electronic Engineers. Eine in den USA ansässige Ingenieurvereinigung zur Erstellung von Standards und Normen.

<sup>2</sup> SNMP Simple Network Management Protocol. Netzwerk-Protokoll das die Verwaltung von Netzwerk-Geräten definiert.

<sup>3</sup> RMON Remote Network Monitoring (RFC1757, RFC2021). Erweiterte SNMP MIB (Management Information Base), die das Sammeln und Abfragen von Ethernet-Leistungsdaten aus der Ferne erlaubt. RMON gliedert die Daten in funktionsorientierte Gruppen wie Statistics, History, Host, HostTopN, etc.

### 3.4.3. Einfache Konfiguration wichtig

Eine weitere häufige Ursache von Ausfällen stellen menschliche Bedienfehler dar. Zum Beispiel kann es schnell passieren, daß ein Administrator den Switch irrtümlich falsch konfiguriert. Insbesondere kleinere Unternehmen sollten deshalb nicht nur auf einen günstigen Preis schauen, sondern bei der Produktauswahl auch Fragen wie einfache Bedienung, Zuverlässigkeit, Support und Sicherheit berücksichtigen.



Einfach ist besser: Leicht verständliche Browser-Oberflächen senken die Wahrscheinlichkeit von Fehlbedienungen.

Als besonders wichtig erweist sich oft der Bedienungsaspekt, denn in kleineren Firmen betreut meist nicht ein spezieller IT-Administrator das Netzwerk. Diese Aufgabe übernehmen in vielen Fällen ein oder zwei "normale" Mitarbeiter, die sich das entweder zutrauen oder diese Aufgabe zugewiesen bekommen haben. Die Implementierung einer ausfallsicheren Netzwerkinfrastruktur erfordert allerdings schon ein gewisses Know-how, das man im Zweifelsfall von einem IT-Dienstleister beziehen sollte.

### 3.5. Betriebssysteme

Es gibt etliche Betriebssysteme für den Netzwerkservers. Eine kostenfreie Variante ist Linux, ein Derivat des großen Bruder Unix. Leider ist dieses Betriebssystem recht schwer zu handhaben, weshalb es nur in größeren Umgebungen oder als Web-Server zum Einsatz kommt. Eine weitere Alternative ist NetWare von Novell. Dieses System hat eine lange Vergangenheit und bedeutend mehr Sicherheitsmechanismen als Windows. Die Kosten sind mit Windows zu vergleichen, die Möglichkeiten weit größer. Leider läßt die Verbreitung von NetWare – noch vor drei Jahren über 90 % aller Server waren mit NetWare versehen – immer stärker nach.

In kleinen und mittleren Umgebungen – und dort, wo es die spezielle Software des Kunden erfordert – setze ich Windows ein. Von den genannten Betriebssystemen ist es mit Sicherheit das schlechteste, aufgrund der schnellen Installation und einfachen Bedienbarkeit aber das preiswerteste.

Für sehr kleine Netze – bis zu 5 PCs – reicht auch ein „normales“ Windows, beispielsweise Windows XP PRO.

### 3.6. Datensicherung

Die Datensicherung ist ein Hauptgrund für die Anschaffung eines Servers. Da die Daten aller Mitarbeiter zentral auf dem Server gespeichert sind, fällt hier die Sicherung besonders einfache aus. Weiterhin muß auch nur ein Gerät angeschafft werden, wodurch auch höherer Komfort durch ein besonders „nettes“ Gerät erreicht wird.

Es gibt mehrere Varianten der Datensicherung:

In kleinen Umgebungen reicht das tägliche Sichern auf eine zweite Festplatte, etwa mit dem von mir entwickelten Programm CyberCopy.

Als Standard für die Datensicherung im Netzwerk haben sich seit geraumer Zeit Bandlaufwerke durchgesetzt. Abhängig von der zu sichernden Datenmenge kommt DAT oder DLT zum Zug. Für diese Bandsicherungen gibt es verschiedene Methoden der Bandaufteilung; näheres zu diesem umfangreichen Thema finden Sie in meinem Essay zur Datensicherung ([www.Cyber-Engineering.de](http://www.Cyber-Engineering.de)).

### 3.7. Netzwerkschutz

Mit einigen kostengünstigen Hilfsmitteln kann ein Firmennetzwerk recht gut vor unbefugten Eindringlingen und möglichen Virenangriffen geschützt werden. Ich führe hier die Fachbegriffe und eine kurze Erklärung auf, Details findet der Leser in meiner Abhandlung zur Sicherheit im Netzwerk. Eine Inhaltsangabe steht unter [www.Cyber-Engineering.de](http://www.Cyber-Engineering.de).

### 3.7.1. Die Firewall

Eine „Feuerwand“ ist in der Regel im Router integriert. Sie bildet den ersten Schutzmechanismus, da sie direkt am Übergang des lokalen Netzwerkes zum Internet sitzt. Diese einzurichten erfordert einiges Fachwissen und ist vom Laien nicht zu bewerkstelligen.

### 3.7.2. Antivirenprogramme

Solche Programme sind für Serverumgebungen zwingend notwendig, da sich Viren in Netzwerken sehr schnell verbreiten. Am Markt gibt es konkurrierende Lösungen, die sich in Güte und Funktion kaum unterscheiden. Besonderes Augenmerk ist hier auf die zentrale Administrierbarkeit und eine Vollautomatik zu legen. Wie auch bei Firewalls ist für die richtige Auswahl sowie die Konfiguration eines solchen Programms erhebliches Fachwissen erforderlich.

Da auch das Thema Viren ein sehr weit gefächert ist, wurde hierzu von mir die Abhandlung *Schutz vor Computerviren* verfaßt, ebenfalls unter [www.Cyber-Engineering.de](http://www.Cyber-Engineering.de) zu finden.

## 4. Netzwerkkommunikation

Bei der Netzwerkkommunikation wird es schnell kompliziert und unübersichtlich. Ich schneide deshalb die wichtigsten Begriffe hier an.

### 4.1. Protokolle

Ein Protokoll ist die Sprache, mit der sich die verschiedenen am Netzwerk teilnehmenden Geräte unterhalten. Von den vielen Protokollen, die in der Vergangenheit aufgetaucht sind, konnten sich nur einige durchsetzen; meist hängen diese Protokolle mit dem Betriebssystem des Servers zusammen.

Natürlich hat auch Microsoft ein eigenes Protokoll entwickelt, daß – ganz Firmenphilosophie – extrem einfach zu bedienen, dafür langsam und störanfällig ist. Es wird nur von Netzwerkanfängern benutzt.

Novell hat in NetWare das Protokoll *IPX/SPX* integriert. Sehr schnell, äußerst stabil und vielseitig im Einsatz war es lange Zeit das führende Protokoll.

Durch das Internet wurde das *TCP/IP* Protokoll populär, daß – da es kostenfrei zu haben war – von Unix und Linux benutzt wird. Es ist mittlerweile das am häufigsten benutzte Protokoll, da jedes Betriebssystem es wegen der Internetanbindung beherrschen muß.

Einziger Außenseiter ist noch Apple: Hier wird Apple-Talk benutzt, eine Sprache, die nur von diesen Maschinen gesprochen und verstanden wird. Die TCP/IP Anbindung erfolgt durch Umrechnung – ein Grund, warum Webseiten auf dem Apple anders aussehen als unter Linux oder Windows.

#### 4.1.1. TCP / IP

Es handelt sich um ein sehr einfaches Protokoll, daß lediglich dazu dient, Daten von Punkt A nach Punkt B zu verschicken. Aufgrund seiner Einfachheit ist dieses Protokoll auch sehr schnell und kaum störanfällig.

##### 4.1.1.1. IP Adressen

Zur Unterscheidung der einzelnen an das Netzwerk angeschlossenen Geräte werden – wie sollte es anders sein – Nummern verwendet. Man nennt diese *IP-Adressen*; sie haben die Form xxx.xxx.xxx.xxx, wobei jedes xxx eine Wert zwischen 0 und 255 annehmen kann. Die Grenzen 0 und 255 sind in der Regel für die Selbstverwaltung des Netzwerkes reserviert und sollten nicht benutzt werden. Jede Nummer darf im Netzwerk nur einmal vergeben sein – ansonsten kommt es zum sogenannten *IP-Konflikt*.

Die IP-Nummer alleine ist noch keine vollwertige Adresse, sie wird ergänzt durch die *Subnetz-Maske*. In der Regel lautet diese 255.255.255.0. Wird diese Maske verändert, wird durch Bitaddition die IP-Nummer verschoben. Dieses für den Laien komplizierte System ist in der einschlägigen Fachliteratur beschrieben.

##### 4.1.1.2. IP Kreise

In mittleren und großen Netzwerken wird die Verteilung der IP-Adressen in IP-Kreisen organisiert; jeder IP-Kreis bildet ein eigenes Netzwerk, daß nur über einen *Gateway* (Übergang) zu erreichen ist.

Als IP-Kreis wird eine Menge an IP-Nummern bezeichnet, bei dem die ersten drei Päckchen der IP Nummern gleich sind, beispielsweise 192.168.1.xxx.

Es wird zwischen lokalen und globalen IP Nummern unterschieden: alle IP-Adressen der Form 192.168.xxx.xxx gelten als lokale IP Bereiche. und werden von Routern nicht weitergegeben – außer man konfiguriert dies extra. Alle anderen Nummernkreise sollten nicht verwendet werden.

#### 4.2. Windowsprotokolle

Um ein reines Windows-Netzwerk aufzubauen, benötigt man eine ganze Menge an Protokollen, die aufeinander aufbauen. Da der Anwendungsbereich von „Windows for Workgroups“ eher in den Privatbereich als „Windows für Wohngemeinschaften“ fällt, sei hier nur dessen Existenz erwähnt.

Gerd Gerhardus

Fachinformatiker für Systemintegration & Anwendungsentwicklung

Gerd Gerhardus studierte Elektrotechnik an der Bergischen Universität Wuppertal und gründete noch während der Studienzeit im Jahre 1994 die Cyber Engineering Gerd Gerhardus. Anfangs war das Unternehmen auf den Vertrieb von Hard- & Software ausgerichtet, entwickelte sich jedoch schnell zum Dienstleister für mittelständische Kunden, insbesondere Handwerkesbetriebe und Steuerkanzleien. Bereits in den Anfängen der Firma legte Gerd Gerhardus höchsten Wert auf schnellen und kompetenten Service, bei dem mit dem Kunden „deutsch“ und kein Fachchinesisch gesprochen wird.

Heute gibt Gerd Gerhardus sein umfangreiches Fachwissen und seine Erfahrungen in Vorträgen und Vorlesungen weiter. Diese werden durch eine Reihe von Publikationen ergänzt. Eine Übersicht ist auf der Firmenhomepage [www.Cyber-Engineering.de](http://www.Cyber-Engineering.de) zu finden.

Durch ständige Erweiterung des Kundenkreises und damit des Unternehmens wuchs auch die Produkt- und Dienstleistungspalette. Die verschiedenen Warenwirtschaftssysteme der Kunden verlangen immer schnellere Server und zuverlässigere Netzwerke, Heimarbeitsplätze werden geschaffen und das Internet gehört zum Standard der Arbeitsumgebungen. Mit der Notwendigkeit, das lokale Netzwerk „an die Welt“ anzuschließen und es dabei sicher zu halten, werden auch die Telefonanlagen in das Sicherheitskonzept eingebunden und selbstverständlich von der Cyber Engineering Gerd Gerhardus geliefert, programmiert und gewartet.

Bald entstand die Nachfrage nach weiter reichenden Sicherheitskonzepten, womit – unterstützt durch den Novell - Fachmann, Elektriker und ausgebildeten Sicherheitstechniker – auch an Server und TK - Anlage angeschlossene Alarmanlagen von der Cyber Engineering Gerd Gerhardus installiert und gewartet wurden.

Durch die lange Berufserfahrung und die sich ständig erweiterten Beziehungen zu weiteren Fachunternehmen fungiert die Cyber Engineering Gerd Gerhardus mittlerweile auch als Übernehmer für Großprojekte.

Seit 2002 bildet Gerd Gerhardus auch aus!

Cyber Engineering  
Gerd Gerhardus

Friedrichstrasse 2  
D - 42 781 HAAN

fon 02129 3 77 77 3  
fax 02129 3 777 66

[www.Cyber-Engineering.de](http://www.Cyber-Engineering.de)  
[Mail@Cyber-Engineering.de](mailto:Mail@Cyber-Engineering.de)

## 5. Anhang

### 5.1. Normen - Grenzwerte für Cat5, Cat6 und Cat7

Elektrische Eigenschaften	Frequenz in MHz	Cat5(e) 2002	Cat6	Cat7
min. Return Loss in dB	1	26,0	30,0	30,0
	100	20,0	24,0	28,0
	250	-	16,0	20,0
	600	-	-	12,4
max. Dämpfung in dB	1	0,1	0,1	0,1
	100	0,4	0,2	0,2
	250	-	0,32	0,32
	600	-	-	0,49
min. NEXT in dB	1	80,0	80,0	80,0
	100	43,0	54,0	73,4
	250	-	46,0	66,4
	600	-	-	60,7
min. PSNEXT in dB	1	77,0	77,0	77,0
	100	40,0	50,0	69,4
	250	-	42,0	63,4
	600	-	-	57,7
min. FEXT in dB	1	65,0	65,0	65,0
	100	35,1	43,1	60,0
	250	-	35,1	54,0
	600	-	-	48,3
min. PSFEXT in dB	1	62,0	62,0	62,0
	100	32,1	40,1	57,0
	250	-	32,1	51,0

## 6. Literaturhinweise

Folgende Publikationen sind von Gerd Gerhardus erschienen und werden ständig aktualisiert:

### 6.1. Internet & Netzwerk

Schutz vor Computerviren und Hackern  
Sicherheit im Netz  
Small LAN - kleine Netzwerke  
Wireless LAN  
Internetzugang  
Pegasus Mail – Das Mailprogramm

### 6.2. Allgemeines

Case Modding (in Vorbereitung)  
CDs und DVDs brennen  
Der Wohnzimmer PC  
Leitfaden zum Computerkauf  
PC im Eigenbau  
Software preiswert  
Texterkennung mit PC und Scanner (in Vorbereitung)  
Windows Registry  
Windows XP - Neuerungen

Alle hier vorgestellten Abhandlungen (und in Zukunft noch einige andere) finden Sie im Internet unter

[www.Cyber-Engineering.de](http://www.Cyber-Engineering.de)

oder

[www.Gerhardus.com](http://www.Gerhardus.com)

In Zukunft können Sie diese auch direkt von dort bestellen; natürlich sind wir auch telefonisch unter

02129 / 3 77 77 3