

# Windows NT

## [Der Versuch einer Zusammenfassung]

Version 1.10 [13.August 2002] stable ;-)

von *ST* für alle die es lesen wollen ...

Windows NT verkörpert heute das, wogegen Unix in den sechziger Jahren angetreten ist. Es hat alle klassischen Probleme von kommerzieller und nicht freier Software.

Inhalt	Seite
<b>1. Grundlagen</b> .....	3
1.01 Daten.....	3
1.02 Ausführungsmodi.....	3
1.03 Architektur.....	3
1.04 Varianten.....	5
1.05 Servicepacks und Hotfixes.....	5
1.06 Dateisystem.....	5
1.07 Systemstart.....	7
1.08 Bootmechanismus.....	7
1.09 Hinweise zur Partitionierung.....	9
1.10 Installationsdisketten erstellen.....	9
1.11 NT von Diskette starten.....	9
1.12 Ereignisanzeige.....	10
1.13 Dienste.....	10
<b>2. Benutzerkonten</b> .....	11
2.01 Typen von Benutzerkonten.....	11
2.02 Vordefinierte Benutzer.....	12
2.03 Vordefinierte Gruppen.....	12
2.04 Vordefinierte lokale Gruppen.....	13
2.05 Erstellen von Benutzerkonten.....	14
2.06 Eigenschaften von Benutzerkonten.....	14
2.07 Eigenschaften von Domänenbenutzerkonten.....	14
2.08 Kennwörter.....	14
2.09 Löschen von Benutzerkonten.....	14
<b>3. Benutzerumgebung</b> .....	15
3.01 Benutzerprofile.....	15
3.02 Basisverzeichnis.....	15
3.03 Anmeldescripte.....	15
3.04 Erstellen von Benutzerprofilen.....	15
3.05 Mögliche Benutzerprofile.....	16
<b>4. Anmeldevorgang anpassen</b> .....	16
4.01 Ändern von Schlüsseln in der Registrierung.....	16
4.02 Schlüssel und mögliche Werte für den Anmeldevorgang..	17
4.03 Beeinflussung des Bildschirmschoners.....	17
<b>5. Der net-Befehl</b> .....	18
5.01 net user.....	18
5.02 net group.....	19
5.03 net send.....	19
<b>6. Suchpfade</b> .....	20
6.01 Suchpfade unter NT.....	20
6.02 Bedeutung der autoexec.bat.....	20

<b>7. Prozesse</b> .....	20
7.01 Vorder- und Hintergrundprozesse.....	20
7.02 Unterschiede in NT.....	21
7.03 Werkzeug für die Prozessverwaltung.....	21
7.04 Prozessattribute.....	21
7.05 Der Schedule Dienst.....	22
<b>8. Dateisystem und Festplattenverwaltung</b> .....	23
8.01 Grundlegende Aufgaben.....	23
8.02 Festplatte Benutzern zur Verfügung stellen.....	23
8.03 Festplattenstandards.....	23
8.031 IDE.....	23
8.032 EIDE.....	24
8.033 SCSI.....	25
8.04 Übersicht Dateisysteme.....	26
8.05 NTFS.....	27
8.06 Formatieren und Verwalten des Dateisystems.....	28
8.07 NTFS Dateisystem erweitern.....	29
<b>9. RAID Systeme</b> .....	30
<b>10. Copyleft, Quellen, Credits, Versionen</b> .....	33
10.01 Copyleft.....	33
10.02 Quellen.....	33
10.03 Credits.....	33
10.04 Versionsänderungen.....	33

Copyright (c) 2002 ST.

Es wird die Erlaubnis gegeben dieses Dokument zu kopieren, verteilen und/oder zu verändern unter den Bedingungen der GNU Free Documentation License, Version 1.1 oder einer späteren, von der Free Software Foundation veröffentlichten Version. Eine Kopie dieser Lizenz ist im Netz unter <http://www.gnu.org/copyleft/fdl.html> zu finden.

Eine deutschsprachige Version gibt es hier:  
<http://nautix.sourceforge.net/docs/fdl.de.html>

Dieses Script gibt es als html- und pdf- Version sowie die Quelldatei als StarOffice Dokument im Netz unter <http://st23.de>

# 1. Grundlagen

## 1.01 Daten

- ➔ 4 GB adressierbarer Speicherraum, davon 3 GB für Anwendungen nutzbar
- ➔ Microkernel wird von teilweise selbstständigen Teilsystemen unterstützt
- ➔ präemptives Multitasking  
[die einem Prozess zugeordnete Zeit wird vom Betriebssystem bestimmt]
- ➔ Multiuser Betriebssystem

## 1.02 Ausführungsmodi

NT unterscheidet zwischen dem Kernel- und dem User Modus.

### Kernel - Modus

Der Kernel - Modus ist ein privilegierter Modus mit uneingeschränktem Zugriff auf die Systemressourcen. Nur Prozesse des Betriebssystems selbst werden in diesem Modus ausgeführt.

### User - Modus

Im User - Modus ist nur indirekter Zugriff auf das System möglich. Ist eine Anforderung an das System erforderlich, entscheidet das Betriebssystem ob der Zugriff gewünscht oder abgelehnt wird.

## 1.03 Architektur

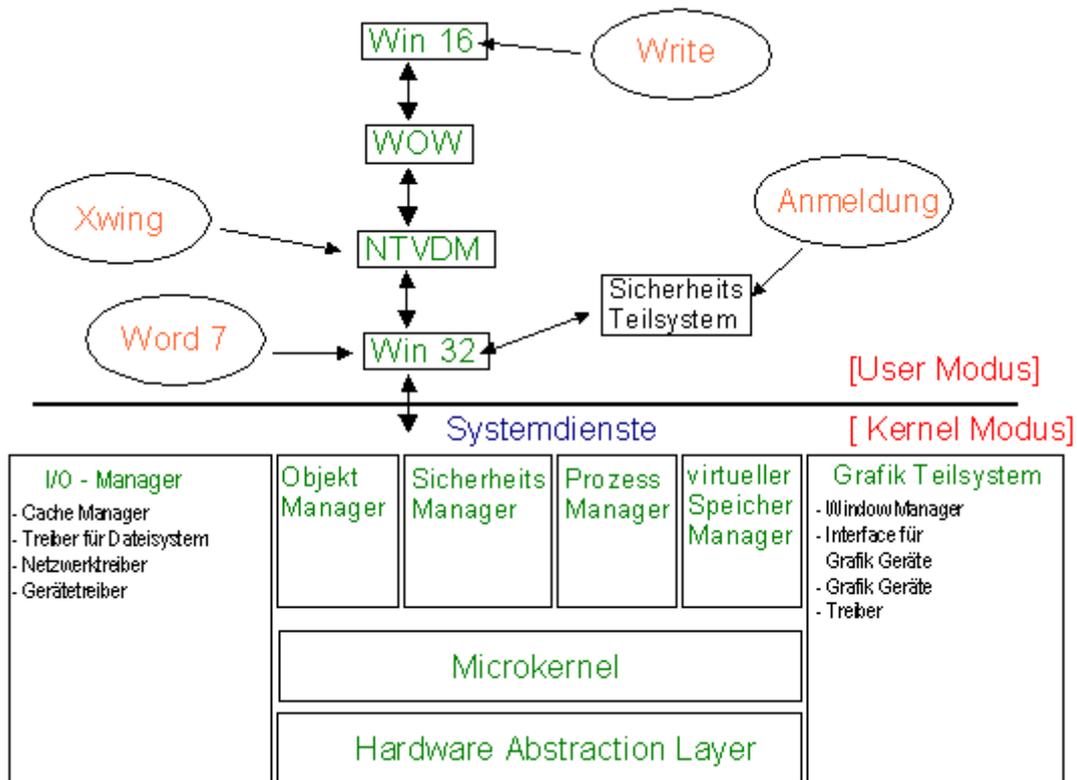


Abbildung 1: Architektur von Windows NT

## Microkernel

➡ Steuerung und Verwaltung aller zugeordneten Teilsysteme

## Hardware Abstraction Layer

➡ Die Kommunikation mit der Hardware erfolgt über ein eigenständiges Teilsystem dem sogenannten Hardware Abstraction Layer [HAL]

## I / O - Manager

➡ steuert die Ein- und Ausgabeoperationen des Systems

## Objekt - Manager

➡ Verwaltung von Systemobjekten [Datenstrukturen für Systemressourcen wie Dateien, Anschlüsse, Prozesse, ...]

## Sicherheits - Manager

➡ Verwaltung des Sicherheitssystems

## Prozess - Manager

➡ erstellt und verwaltet Systemprozesse

## virtueller Speicher - Manager

➡ Verwaltung des Systemspeichers

## Grafik Teilsysteme

➡ Schnittstelle zur grafischen Anzeige

Die **Teilsysteme** stellen Systemdienste zur Verfügung mit deren Hilfe die Anforderungen seitens des User - Modus bearbeitet werden können.

## Win 32 Teilsystem

Das Win 32 Teilsystem stellt Prozesse für Anwendungsprogramme über die Standardschnittstelle [API Application Programming Interface] zur Verfügung. Die API ist eine Sammlung von Standard Bibliotheksroutinen. Das Win 32 Teilsystem kann von echten 32 Bit Anwendungen direkt genutzt werden.

## Win 16 Teilsystem

Das Win 16 Teilsystem ist für DOS und 16 Bit Anwendungen. Sie werden von einem Satz verschachtelter Teilsysteme verwaltet, diese greifen dann auf das Win 32 Teilsystem zu. 16 Bit Anwendungen werden mit Hilfe des **WOW** [Win on Win 32] - Teilsystems in entsprechende 32 Bit Aufrufe konvertiert.

## NTVDM - NT Virtual DOS Maschine

Mit dem NTVDM werden eventuell notwendige DOS Dienste zur Verfügung gestellt. Reine DOS Anwendungen können direkt auf NTVDM zugreifen.

## 1.04 Varianten

### **NT - Workstation**

NT - Workstation regelt im wesentlichen die Arbeitsweise eines Einzelplatzcomputers und ist im Netzwerk als Workgroup - Modell verfügbar.

### **NT - Server**

Für den Einsatz als Server vorgesehen. Rechner können zu Gruppen zusammengefasst werden. Eine solche Gruppe wird dann als Domäne bezeichnet. NT - Server kann PDC [Primary Domain Controller] und BDC [Backup Domain Controller] zur Verfügung stellen.

**Hinweis:** Domäne bitte nicht mit Arbeitsgruppe oder Workgroup verwechseln !

In einer Arbeitsgruppe oder Workgroup müssen die Benutzer auf allen Rechnern im Netzwerk angelegt werden an denen sie sich anmelden wollen bzw. auch auf den Maschinen auf die sie zugreifen wollen. Die Benutzer werden auch auf den entsprechenden Rechnern verwaltet. Zur Verwaltung einer Domäne ist ein PDC erforderlich mit dem die Benutzer im Netzwerk verwaltet werden können. Ein Benutzer muss sich nur an der Domäne anmelden um alle für ihn bestimmten Ressourcen zu nutzen. Der Vorteil liegt auf der Hand. Zentrale Administrierbarkeit des Netzwerkes. Eine Domäne ist als logische Strukturierung unabhängig von der tatsächlichen physischen Struktur des Netzwerkes zu verstehen.

## 1.05 Servicepacks und Hotfixes

**Servicepacks** enthalten Korrekturen und Verbesserungen für das Betriebssystem. Service Packs sollten immer installiert werden, da sie Sicherheits-, Stabilitäts- und Kompatibilitätstechnisch sehr relevant sind. Das letzte Servicepack für NT 4.0 ist das SP 6a (128 Bit). Die Weiterentwicklung von NT 4.0 wurde damit abgeschlossen. Die NT 4.0 Servicepacks sind kumulativ aufgebaut, das bedeutet SP 2 beinhaltet SP1. Servicepacks sollten nach jeder Hard- und Softwareveränderung neu installiert werden, besonders wenn nach der NT Installations CD gefragt wurde.

**Hotfixes** sind Fehlerbehebungen, sie sind die Reaktion auf kritische Fehler bzw. Sicherheitslücken die schnellstmöglich behoben werden müssen. Hotfixes sind nicht getestet und sollten nur eingesetzt werden wenn der entsprechende Fehler wirklich vorhanden ist und das Hotfix notwendig ist.

## 1.06 NT-Dateisystem

Die "Standard" Dateistruktur von NT.

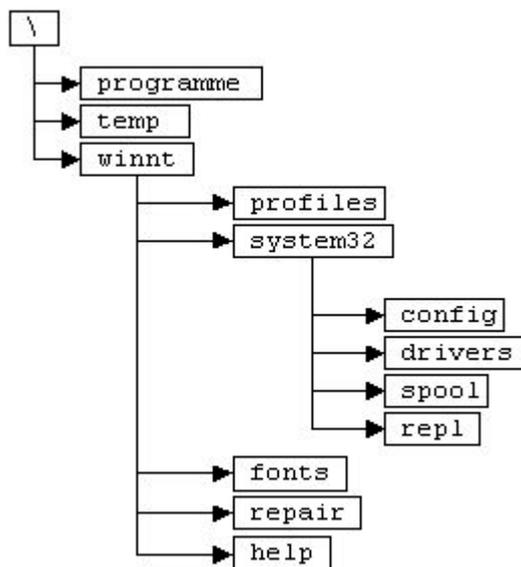


Abbildung II:Dateistruktur

### **programme**

- ➔ ausführbare Dateien für NT
- ➔ Anwendungen

### **temp**

- ➔ Verzeichnis für temporäre Dateien

### **winnt**

- ➔ Systemdateien
- ➔ Der Verzeichnispfad wird in der Systemvariablen %systemroot% abgelegt. Es ist also das default Systemverzeichnis. Bei der Erstellung von Scripten ist dies besonders wichtig, da man %systemroot% als Pfadangabe nutzen kann.

### **profiles**

- ➔ Verzeichnis für Benutzerprofile
- ➔ ein Benutzerprofil wird in der Benutzerumgebung definiert

### **system32**

- ➔ ausführbare Dateien von Win NT
- ➔ dynamic link librarys (dll's)
- ➔ teilweise Konfigurationsdateien

### **config**

- ➔ Registrierungsdateien
- ➔ Ereignisprotokolle
- ➔ Datenbank für Benutzer und Gruppenkonten

### **drivers**

- ➔ Gerätetreiber

### **spool**

- ➔ Verwaltung der Spooldateien des Druckteilsystems

## repl

- ➔ Replikation
- ➔ Ausgangsverzeichnis für der Replikationsdienst

## fonts

- ➔ Schriftarten

## repair

- ➔ Daten für die Notfalldiskette

## help

- ➔ Hilfesystem

Windows NT nutzt zur Identifikation von Dateien auch die UIN [Uniform Naming Convention]

\\Rechner\Verzeichnispfad\Datei

z.B.

\\server02\home\st\distributed\rc5\rc.exe

## 1.07 Systemstart

Das Laden von NT erfolgt in mehreren Schritten. NT installiert defaultmäßig ein Bootmenü, dort können auch [wenn vorhanden] weitere Betriebssysteme integriert werden.

- ➔ 1. Wahl des zu startenden Betriebssystems aus dem Bootmenü  
NT richtet standardmäßig 2 Bootmodi ein "normal" und "vga-modus".
- ➔ 2. Auswahl des Hardwareprofiles
- ➔ 3. Überprüfung der Hardwarekonfiguration
- ➔ 4. Laden und starten des Kernels [ntoskrnl.exe]  
Der Kernel liegt unter %systemroot%\system32. Der Kernel liegt immer auf der NT Partition, auch wenn dies nicht die aktive Partition des Systems ist.
- ➔ 5. Starten aller weiteren Prozesse bzw. Dienste.

## 1.08 Bootmechanismus

- ➔ bootloader lokalisiert den MBR [Master Boot Record] [Spur 0 Sector 0]
- ➔ erkennen der Systempartition [aktive Partition]
- ➔ Ausführung des eigentlichen Ladeprogrammes [ntldr]. Dieses liegt im Hauptverzeichnis der **aktiven** Partition, das muss nicht die NT Partition sein. Ntldr benutzt für den weiteren Systemstart zwei Dateien, die sich ebenfalls auf der Systempartition befinden boot.ini und ntdetect.com.

## ntdetect.com

- ➡ wird von ntldr ausgeführt nachdem ein Hardwareprofil ausgewählt wurde
- ➡ ntdetect.com überprüft die Hardwarekonfiguration

## boot.ini

- ➡ legt das Bootmenü fest, dass mit Hilfe von ntldr angezeigt wird
- ➡ die boot.ini ist eine ASCII-Datei (read only)
- ➡ sie liegt in der Systempartition

Die boot.ini besteht aus 2 Sektionen, bootloader und operating system.

[bootloader]

Parameter	Beschreibung
timeout	legt die Anzahl Sekunden fest die dem Benutzer zur Auswahl bleiben
default	enthält den Pfad zum Standard Betriebssystem, dieses wird automatisch nach "timeout" gestartet

[operating system]

Hier befindet sich die Liste der verfügbaren Betriebssysteme. Ein Eintrag umfasst den Pfad zur Bootpartition des Betriebssystems, die am Bildschirm anzuzeigende Zeichenfolge und eventuell optionale Parameter.

### Formulierung der Pfadangabe

Diese Angaben gelten nur für IDE Platten nicht für SCSI Geräte.

IDE - Integrated Device Equipment

SCSI - Small Computer System Interface

*multi(m)disk(x)rdisk(n)partition(p)\verzeichnis="text" [/parameter]*

m	Nummer des IDE Controllers, der erste hat den Wert 0
x	wird für multi (also IDE) nicht verwendet und ist immer 0
n	Nummer der Festplatte an diesem Controller, beginnt bei 0
p	Nummer der Partition, beginnt bei 1

### Beispiel einer boot.ini

[boot loader]

timeout=30

default=multi(0)disk(0)rdisk(0)partition(2)\WINNT

[operating systems]

multi(0)disk(0)rdisk(0)partition(2)\WINNT="Windows NT Workstation, Version 4.0"

multi(0)disk(0)rdisk(0)partition(2)\WINNT="Windows NT Workstation, Version 4.0 [VGA-Modus]" /basevideo /sos

C:\ = "Microsoft Windows"

## 1.09 Hinweise zur Partitionierung

Das Tool fdisk von Windows 95/98 erkennt keine NTFS Partitionen und kann also mit ihnen auch nicht umgehen.

Man unterscheidet zwischen primären und erweiterten Partitionen. NT kann bis zu 4 Partitionen pro Platte verwalten. Möglich sind 4 primäre oder 3 primäre und eine erweiterte Partition. Es kann nur eine erweiterte Partition pro Platte erstellt werden, diese kann dann aber in mehrere logische Laufwerke unterteilt werden. Die Laufwerksbuchstaben werden zuerst den primären Partitionen und dann den erweiterten Partitionen bzw. logischen Laufwerken zugewiesen. Während der Installation von NT ist es möglich die Festplatte zu partitionieren.

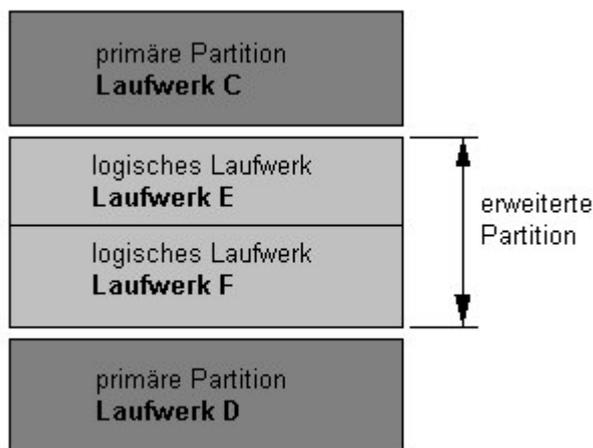


Abbildung III:Beispielpartitionierung

## 1.10 Installationsdisketten erstellen

Die drei Installationsdisketten kann man mit jedem Windows erstellen. Sie liegen auf der NT Installations CD unter \i368\winnt. Mit dem Parameter /ox können sie erstellt werden.

z.B. D:\i368\winnt /ox

[wenn D: das CD-ROM Laufwerk ist in dem sich die Installations CD befindet]

## 1.11 NT von Diskette starten

### **Bootdisk erstellen:**

Eine Diskette mit NT formatieren, nicht mit einem anderen Betriebssystem, da die Diskette sonst nicht bootfähig ist [z.B. bei Win 95/98].

folgende Dateien auf die Diskette kopieren:

- ➡ boot.ini
- ➡ ntldr
- ➡ ntdetect.com
- ➡ bootsect.dos (Bootmanager)

Diese Diskette reicht nun aus um NT zu starten, solange der Kernel [ntoskernel] noch verfügbar ist. Er liegt unter \winnt . Ist dies nicht der Fall, so ist die Diskette unbrauchbar, das NT dann aber auch. Viel Spass bei der Neuinstallation ;-).

## 1.12 Ereignisanzeige

Die Ereignisanzeige zeigt das Protokoll über den Betriebszeitraum, seit dem ersten Systemstart, wenn es nicht zwischenzeitlich gelöscht wurde.

### **mögliche Nachrichten:**

- ➔ Systembezogene Nachrichten [von Teilsystemen und Gerätetreibern erzeugt]
- ➔ Sicherheitsbezogene Nachrichten
- ➔ Anwendungsbezogene Nachrichten

### **Symbole**

	Information, Statusmeldung
	Fehler, Ausfall einer Systemkomponente oder eines Teilsystems
	Warnung, unkritischer Fehler von Systemkomponenten

Die Symbole sind von Windows 2000, die von NT sehen aber ähnlich aus.

## 1.13 Dienste

Die Dienste können grafisch unter Systemsteuerung/Dienste [NT-Workstation] bzw. Servermanager [NT-Server] administriert werden.

Sie können aber auch per net Kommando verwaltet werden.

net start	zeigt eine Liste aller aktuell ausgeführten Dienste
net start parameter	Dienst starten
net stop parameter	Dienst beenden
net pause parameter	Dienst anhalten
net continue parameter	Dienst fortfahren
net /help	Hilfe mit ausführlichen Erklärungen

## 2. Benutzerkonten

Mit Hilfe eines Benutzerkontos identifiziert sich ein Benutzer gegenüber dem System und erhält dadurch Zugriff auf Ressourcen.

Benutzerkonten besitzen neben dem Benutzernamen weitere Eigenschaften :

- ➔ Mitgliedschaft in einer oder mehreren Gruppen
- ➔ Kennwort und Regeln zur Verwaltung des Kennwortes
- ➔ gültige Anmeldezeiten und Arbeitsstationen
- ➔ Einwählrechte (z.B. Internet)
- ➔ Benutzerumgebung
- ➔ Basisverzeichnis
- ➔ Satz von Privilegien (Benutzerrechte)

### **Grundlagen für Benutzerkonten**

Benutzerkonten werden durch einen Namen identifiziert. Für diesen gelten folgende Regeln:

- ➔ maximal 20 Zeichen lang
- ➔ Groß- und Kleinschreibung möglich (keine Differenzierung durch das System)
- ➔ Zeichen und Ziffern erlaubt
- ➔ Eingebundene Leerzeichen sind möglich
- ➔ Namen müssen eindeutig sein

### 2.01 Typen von Benutzerkonten

#### **Domänenbenutzerkonten** (Globale Benutzerkonten)

Eine Domäne ist eine Zusammenfassung von vernetzten Rechnern, die an demselben Sicherheitssystem teilnehmen. Der Benutzer identifiziert sich mit Hilfe eines solchen Kontos gegenüber der Domäne und erhält Zugriff auf Domänenressourcen. Ein Benutzer kann sich von jedem Rechner des Netzwerkes (Domäne) an der Domäne unter demselben Namen und mit seinem Kennwort anmelden. Domänenbenutzerkonten werden in der sogenannten master-directory-database auf dem PDC abgelegt.

#### **Lokale Benutzerkonten**

Umfasst die Informationen durch die sich ein Benutzer dem lokalen Rechner gegenüber identifiziert um Zugriff auf lokale Ressourcen zu erhalten. Um Zugriff auf Ressourcen eines anderen Rechners zu erhalten, muss der Benutzer über ein gesondertes Benutzerkonto auf dem anderen Rechner verfügen. Üblicherweise werden lokale Benutzerkonten im Rahmen des Workgroup Modells verwendet.

#### **Windows NT Gruppen**

Eine Sammlung von Benutzerkonten denen identische Zugriffsrechte auf Dateien und Ressourcen vergeben werden.

**Globale Gruppen** dienen der Organisation von Domänenbenutzerkonten.

**Lokale Gruppen** ermöglichen den Zugriff auf Netzwerkressourcen des lokalen Rechners. Die Einstellungen für die Benutzerkonten werden als binär codierte Dateien in der Datenbank des Sicherheitskontenmanagers (SAM - Security Account Manager) abgelegt.

%systemroot%\system32\config

## 2.02 Vordefinierte Benutzer

### **Administrator**

- ➔ Konto für die Systemverwaltung
- ➔ kann sich selbst den Vollzugriff auf Ressourcen und das Dateisystem erteilen
- ➔ mächtigstes Konto
- ➔ aus Sicherheitsgründen mindestens ein weiteres Adminkonto anlegen
- ➔ Passwort ist erforderlich
- ➔ jeder der administrative Aufgaben ausführen muss sollte ein eigenes Administratorkonto erhalten

### **Gast**

- ➔ für gelegentliche Benutzer gedacht
- ➔ sollte wenn es nicht gebraucht wird deaktiviert werden
- ➔ Passwort ist erforderlich
- ➔ Veränderung des Passwortes durch den Benutzer sollte verhindert werden

### **System**

- ➔ kann nicht für interaktive- oder Netzwerkanmeldungen verwendet werden
- ➔ Pseudokonto unter dem viele Serverdienste ausgeführt werden
- ➔ besitzt viele Dateirechte

## 2.03 Vordefinierte Gruppen

Globale und jeder Domäne zugeordnete Gruppen:

### **Domänen - Administratoren**

- ➔ Mitglieder dieser Gruppe besitzen Administratorrechte
- ➔ standardmäßig ist das Administratorkonto Mitglied dieser Gruppe

### **Domänen - Benutzer**

- ➔ Mitglieder sind alle globalen Benutzerkonten

### **Domänen - Gäste**

- ➔ enthält das Gastkonto als Mitglied

## 2.04 Vordefinierte lokale Gruppen

### **Administratoren**

- ➡ Mitglieder besitzen Administratorrechte
- ➡ standardmäßig ist das Administratorkonto und die globale Gruppe Domänen - Administratoren als Mitglied enthalten

### **Benutzer**

- ➡ standardmäßig ist die globale Gruppe Domänen - Benutzer Mitglied

### **Gäste**

- ➡ enthält das Gastkonto

### **Hauptbenutzer**

- ➡ Mitglieder können Ressourcen im Netzwerk für andere Benutzer freigeben

Die folgenden Gruppen enthalten standardmäßig keine Mitglieder.

### **Konten Operatoren**

- ➡ Benutzerverwaltung

### **Sicherungs Operatoren**

- ➡ Datensicherung
- ➡ Archivierung

### **Druck Operatoren**

- ➡ Netzwerkdruck

Es gibt noch weitere lokale Gruppen, aber sie alle zu nennen würde den Grundlagenteil unnötig aufblähen.

Gruppen die im Benutzermanager *nicht* angezeigt werden:

### ➡ **Interaktiv**

### ➡ **Netzwerk**

### ➡ **Jeder**

ermöglicht den Zugriff auf Ressourcen für angemeldete Benutzer

## 2.05 Erstellen von Benutzerkonten

Benutzer können mit den grafischen Tools "Benutzermanager für Domänen" (usrmgr) und "Benutzermanager" (musrmgr) erstellt werden. Einfach zusammenklicken ;-). Benutzerkonten können auch durch kopieren eines bestehenden Kontos erstellt werden.

## 2.06 Eigenschaften von Benutzerkonten

- ➔ **vollständiger Name**
- ➔ **Beschreibung**
- ➔ **Kennwortbehandlung**
- ➔ **Gruppenzugehörigkeit**
- ➔ **Profil** (bestimmt die Eigenschaften der Startumgebung)
- ➔ **RAS remote access service** (Einstellungen für Wählverbindungen)

## 2.07 Eigenschaften bei Domänenbenutzerkonten

Domänenbenutzerkonten beinhalten die Eigenschaften der "normalen" Benutzerkonten und zusätzlich folgende:

### **Zeiten**

- ➔ bestimmt zu welchen Zeiten sich ein User anmelden darf

### **Anmelden an**

- ➔ legt fest an welchen Maschinen sich der Benutzer anmelden darf

### **Konto**

- ➔ ermöglicht das Festlegen eines Ablaufdatums für ein Konto

## 2.08 Kennwörter

- ➔ es wird zwischen Groß - und Kleinschreibung unterschieden
- ➔ erlaubt sind Buchstaben Ziffern und Symbole
- ➔ keine Tastenkombinationen mit [Alt] oder [Win] nutzen
- ➔ maximale Länge 14 Zeichen
- ➔ die Speicherung erfolgt in codierter Form in der Benutzerkontendatenbank

## 2.09 Löschen von Benutzerkonten

- ➔ jedes Konto besitzt eine eindeutige ID
- ➔ wird ein Konto gelöscht, so wird auch seine ID gelöscht, diese wird nie wieder verwendet
- ➔ Es ist also nicht möglich ein 100%ig identisches Konto zu erstellen
- ➔ bei Unsicherheit, das Konto nur deaktivieren und nicht löschen

## 3. Benutzerumgebung

### 3.01 Benutzerprofile

- ➔ gespeicherte Sammlung von Systemeinstellungen für das Aussehen des Desktops
- ➔ innerhalb einer Domäne verfügt jeder Benutzer an jeder NT-Maschine an der er sich anmelden darf, über seine vertraute Benutzerumgebung

### 3.02 Basisverzeichnis

- ➔ ein dem Benutzer zugeordnetes Verzeichnis
- ➔ dieses Verzeichnis soll zum Speichern aller vom Benutzer erzeugten Daten verwendet werden

### 3.03 Anmeldescripte

- ➔ werden bei der Anmeldung automatisch ausgeführt
- ➔ meist Stapelverarbeitungs- oder Scriptdatei
- ➔ Pfadangaben werden relativ zu folgendem Verzeichnis interpretiert  
%systemroot%\system32\repl\import\scripts (das bedeutet es kann keine absolute Pfadangabe gemacht werden)
- ➔ Anmeldescripte verändern die Umgebung für spätere Benutzerprozesse nicht (das Setzen von Umgebungsvariablen ist also nur sinnvoll wenn diese bei der Ausführung des Scriptes nötig sind)

*Nutzung von Umgebungsvariablen Anmeldescripten*

- ➔ **%username%**  
enthält den Namen des Benutzerkontos
- ➔ **%homedrive%**  
enthält die Laufwerksspezifikation des Basisverzeichnisses des Benutzers
- ➔ **%homepath%**  
enthält den vollständigen Pfad zum Basisverzeichnis des Benutzers

### 3.04 Erstellen von Benutzerprofilen

- ➔ ein Pfad für die Lage des Profils ist erforderlich
- ➔ dies kann ein lokales Verzeichnis oder eine Freigabe sein
- ➔ bei der Verwendung von Freigaben muss die Angabe in UNC-Schreibweise erfolgen
- ➔ falls kein Benutzerprofil vorhanden ist, wird bei der ersten Anmeldung ein Profil angelegt. Dieses ist dann eine Kopie des Standardbenutzerprofils. Dieses liegt unter %systemroot%\profiles\defaultuser (sollte man sich mal anschauen)

## 3.05 Mögliche Benutzerprofile

### lokale Benutzerprofile

➡ existieren nur auf der lokalen Maschine und werden auch nur hier verwendet

### servergespeicherte Benutzerprofile

➡ werden in ein über das Netzwerk erreichbares Verzeichnis gespeichert

➡ dieses Profil wird an jedem Rechner verwendet an dem sich der User anmeldet, insofern das Verzeichnis mit dem Profil erreichbar ist

➡ servergespeichertes Profil **erstellen**:

➡ Freigabe kontrollieren: %systemroot%\profiles muss freigegeben sein, notwendige Rechte müssen bestehen

➡ bestehendes Profil kopieren

➡ kopiertes Profil einem Benutzerkonto oder einer Gruppe zuordnen (den entsprechenden Pfad angeben)

➡ als Benutzer anmelden und das Profil wunschgemäß anpassen

### verbindliches Benutzerprofil

➡ besondere Art eines Servergespeicherten Profils

➡ es ist schreibgeschützt und kann vom User nicht verändert werden

➡ ist das Verzeichnis nicht verfügbar, kann sich der User nicht anmelden

Beim Anmelden werden servergespeicherte und verbindliche Benutzerprofile auf den Rechner kopiert an dem sich der Benutzer anmeldet. Veränderungen an einem servergespeicherten Profil werden lokal und auf dem Server gespeichert. Servergespeicherte und verbindliche Profile befinden sich in der Regel auf dem PDC bzw. auf der als PDC arbeitenden Maschine.

## 4. Anmeldevorgang anpassen

### 4.01 Ändern von Schlüsseln in der Registrierung

Zum editieren der Registry bietet sich das Tool Regedit an. Man sollte in der Registry nur Schlüssel und Werte verändern wenn man sich 100%ig im Klaren ist was diese Werte und Schlüssel bewirken. Die unter Windowsusern beliebte try & error Methode kann zum Verlust des Betriebssystems und der gespeicherten Daten führen. Wer sich jedoch intensiv mit den Funktionen der Registry beschäftigt, kann sich ein schönes und optimiertes Betriebssystem zusammenschrauben. Herr google hilft in jedem Falle weiter.

Die hier besprochenen Schlüssel sind alle unter folgendem Pfad zu finden:

HKEY\_LOCAL\_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\_NT\CURRENT\_VERSION\WINLOGON

[HKEY -> handle key]

## 4.02 Einige Schlüssel und mögliche Werte für den Anmeldevorgang

### ***DontDisplayLastUserName***

- ➡ legt fest ob das Anmeldefenster den letzten Benutznamen anzeigen soll oder nicht
- ➡ mögliche Werte: 0 und 1 (Zeichenkette); default: 1

### ***ShutdownWithoutLogon***

- ➡ legt fest ob das Anmeldefenster die Schaltfläche Herunterfahren beinhalten soll oder nicht
- ➡ mögliche Werte: 0 und 1; default: 1 NT-Workstation, 0 NT-Server

### ***LegalNoticeCaption und LegalNoticeText***

- ➡ Diese beiden Schlüssel mit Ihren Werten ermöglichen es nach dem Anmelden ein Informationsfenster anzuzeigen.
- ➡ LegalNoticeCaption enthält den Titelzeilentext z.B. "Achtung"
- ➡ LegalNoticeText enthält den Text in der Box z.B. "Einige zur Systemstabilität beitragenden Prozesse konnten nicht initialisiert werden. Bitte starten Sie den Computer neu um das Problem zu beheben."
- ➡ die Nachricht kann dann mit OK weggeklickt werden

### ***RunLoginSkriptSync***

- ➡ legt fest, ob das Anmeldeskript beendet sein muss, bevor dem Benutzer Zugriff auf das System gewährt wird
- ➡ mögliche Werte: 0 und 1; default: 0

## 4.03 Beeinflussung des Bildschirmschoners

Schlüssel: HKEY\_USERS\DEFAULT\CONTROLPANEL\DESKTOP

mögliche Werte:

### ***screensave.exe***

- ➡ legt den gewünschten Bildschirmschoner fest
- ➡ Bildschirmschoner liegen unter %systemroot%\system32 [\* .scr]
- ➡ default: logon.scr

### ***ScreenSaveTimeout***

- ➡ legt fest wann der Bildschirmschoner aktiviert wird (in sekunden)
- ➡ default: 900

### ***ScreenSaveActive***

- ➡ legt fest ob der Bildschirmschoner gestartet werden soll wenn niemand angemeldet ist
- ➡ Werte: 0 und 1 ; default: 0

## 5. net-Befehl

### 5.01 net user

- ➡ ermöglicht das Verwalten von Benutzerkonten
- ➡ Syntax: `net user [username] [*|Kennwort] [Optionen]`
- ➡ `net user` -> zeigt alle derzeit verfügbaren Benutzerkonten an
- ➡ `net user username` -> zeigt alle Daten des entsprechenden Kontos
- ➡ `net user /help` und `net user /?` -> Hilfesystem

mögliche Optionen:

Befehl	Beschreibung [Beispiel]
/add	Konto hinzufügen [ <code>net user st /add</code> ]
*/add	* bewirkt, dass der Benutzer beim ersten Anmelden das Passwort ändern muss [ <code>net user st */add</code> ]
/delete	Konto löschen [ <code>net user st /delete</code> ]
/active:yes/no	aktiviert bzw. deaktiviert das entsprechende Konto [ <code>net user st /active:no</code> ] default ist yes
/comment:"text"	legt die Beschreibung des Kontos fest [ <code>net user st /comment:"no comment"</code> ]
/expires:date/never	legt fest wann das Konto ablaufen soll [ <code>net user st /expires:01.01.2023</code> ] am 01.01.2023 [ <code>net user st /expires:never</code> ] niemals
/fullname:"name"	zum angeben des vollständigen Benutzernamens [ <code>net user st /fullname:"ST The Illumination"</code> ]
/homedir:Pfad	legt das Basisverzeichnis des Benutzers fest [ <code>net user st /homedir:c:\users\st</code> ]
/passwordchg:yes/no	bestimmt ob der user sein Passwort ändern darf [ <code>net user st /passwordchg:no</code> ] default:yes
/passwordreg:yes/no	bestimmt ob der Benutzer ein Passwort besitzen muss [ <code>net user st /passwordreg:no</code> ] default:yes
/profilepath:Pfad	bestimmt die Lage des Profils [ <code>net user st /profilepath:c:\users\st\profile</code> ]
/scriptpath:Pfad	bestimmt die Lage des Anmeldescripts relativ zu %systemroot%\system32\repl\import\scripts [ <code>net user st /scriptpath:st.bat</code> ]
/times:Zeiten/all	legt die Anmeldezeiten des users fest [ <code>net user st /times:mo-mi, 6-18, do, 7-20</code> ] default:all
/workstations:Computer/*	bestimmt an welchen Maschinen sich der user anmelden darf default:* (alle Maschinen) [ <code>net user st /workstations:wkstat1, wkstat3</code> ]

**Beispiel:**

Es soll ein neues Benutzerkonto für Tyler Durdan erstellt werden.

Beim ersten Anmelden muss er ein neues Passwort festlegen.

Das Konto soll am 01.07.2010 ablaufen

Profilpfad:c:\users\durdan

Anmeldescriptpfad:\%systemroot%\system32\repl\import\scripts\durdan.bat

**Befehl:** (das ist ein Befehl, also alles hintereinander schreiben)

```
net user durdan */add /fullname:"Tyler Durdan" /expires:01/07/2010
/profilepath:c:\users\durdan /scriptpath:durdan.bat
```

## 5.02 net group

Die Befehle *net group* und *net local group* ermöglichen es Gruppen zu Verwalten.

**net group Gruppenname**

➡ zeigt die Mitglieder der Gruppe an

**net group chaos /add**

➡ erstellt die Gruppe chaos (leer und ohne Rechte)

**net group chaos st tyler /add**

➡ fügt der Gruppe chaos die Benutzer st und tyler hinzu

**net group chaos st /delete**

➡ entfernt den Benutzer st aus der Gruppe chaos

## 5.03 net send

Syntax: *net send Ziel "Nachricht"*

**mögliche Ziele**

➡ Benutzername

➡ Computername

➡ \* [bedeutet an alle]

➡ /users [an alle lokal angemeldeten Benutzer]

**Beispiel:**

```
net send durdan "Hi Tyler ! Morgen 20:00 Kino ?"
```

**Definitionen von Namen für den Nachrichteneingang:**

Syntax: *net name [Name] [/Optionen]*

Wenn der Benutzer Hans-Joachim gern auch als HaJo erreichbar sein möchte, dann gibt er einfach *net name HaJo /add* ein. Mit *net name* kann man also zusätzliche Empfängernamen definieren.

*net name* - zeigt alle zur Zeit definierten Namen an

*net name Name /add* - definiert einen zusätzlichen Namen

*net name Name /delete* - löscht einen definierten Namen

## 6. Suchpfade

### 6.01 Suchpfade unter NT

NT benutzt zum Auffinden von ausführbaren Dateien Suchpfade. Ein Suchpfad wird als Liste von Verzeichnissen formatiert. Die Suchpfade werden in der Systemvariablen PATH gespeichert. Die Elemente eines Suchpfades können als Laufwerksspezifikation mit einem Verzeichnis und in UNC-Schreibweise angegeben werden. Die Suche beginnt im aktuellen Verzeichnis (defaultmäßig) und erfolgt dann weiter in der Reihenfolge der PATH Variablen. Ausführbare Dateien werden mit Hilfe des Suffix erkannt. In der Variablen PATHEXT werden die als ausführbar vermerkten Dateinamenerweiterungen abgelegt. PATHEXT ist eine Suffixliste. Trennzeichen ist das Semikolon (;) Bsp: .exe; .com; .cmd; ... .

NT verwendet 2 Suchpfade:

- ➡ 1. Systemsuchpfad (PATH) - wird von jedem Benutzer verwendet
- ➡ 2. individueller Suchpfad - kann für jedes Benutzerkonto existieren

Der tatsächliche Suchpfad eines Benutzers setzt sich aus dem Systemsuchpfad und dem individuellen Suchpfad zusammen.

### 6.02 Bedeutung der autoexec.bat

Sie ist für NT nicht zwingend erforderlich und liegt im root-Verzeichnis [\\] der Systempartition. Die Nutzung unter NT erfolgt nur aus Kompatibilitätsgründen (auch wenn es komisch klingt NT und kompatibel in einem Satz zu erwähnen). Bei der Anmeldung werden die PATH-Definitionen der autoexec.bat dem NT Suchpfad hinzugefügt (defaultmäßig). Diese Option kann in der Registrierung geändert werden.

HKEY\_CURRENT\_USER\SOFTWARE\MICROSOFT\WINDOWS\_NT\CURRENT\_VERSION\WINLOGON

Wert: **parse autoexec** Inhalt: 1 (default) [Zeichenfolge] -> 0 führt dazu das die autoexec.bat zukünftig ignoriert wird (siehe oben).

## 7. Prozesse

### 7.01 Vorder- und Hintergrundprozesse

Wenn eine Anwendung gestartet wird, wird mindestens ein Prozess gestartet. Dieser Prozess ist einer Anmeldesitzung zugeordnet. Ein solcher Prozess wird als interaktiver Prozess bezeichnet der über Eingabegeräte z.B. Maus und Tastatur mit dem Benutzer kommuniziert. Solche interaktiven Prozesse laufen im Vordergrund ab. Vordergrundprozesse behalten die Kontrolle über die Anmeldesitzung bis die Aktion erledigt ist oder der Prozess anderweitig beendet wird. Hintergrundprozesse laufen unabhängig von einer Anmeldesitzung. Ein Hintergrundprozess ist unabhängig von weiteren Benutzereingaben. Zur Planung von Hintergrundprozessen ist unter NT der Schedule-Dienst erforderlich.

## 7.02 Unterschiede in NT

Ein interaktiver Vordergrundprozess kontrolliert nur das Fenster in dem er ausgeführt wird und nicht die gesamte Anmeldesitzung. Es können mehrere solcher Prozesse gleichzeitig existieren und der user kann [meistens ;-)] zwischen den Prozessen wechseln.

Hintergrundprozesse können mit der aktuellen Anmeldesitzung in Interaktion treten.

## 7.03 Werkzeug für die Prozessverwaltung

Das Standardwerkzeug für die Prozessverwaltung ist der Task-Manager. Er kann mit [Ctrl]+[Alt]+[Entf] und dann Task-Manager anklicken oder direkt mit [Ctrl]+[Shift]+[Esc] aufgerufen werden.

### **Der Taskmanager**

#### ➡ 1. Anwendungen

Listet die derzeit ausgeführten Anwendungen auf, die Schaltfläche *Task beenden* bricht das markierte Programm ab, *wechsel zu* aktiviert das entsprechende Programm.

#### ➡ 2. Prozesse

Liste alle ausgeführten Prozesse.

#### ➡ 3. Systemleistung

Anzeige der Systemauslastung [Speicher/Prozesse].

## 7.04 Prozessattribute

#### ➡ PID

numerische Prozess ID

#### ➡ Zugriffs-Token

Spezifiziert Daten die sich auf Dateiberechtigungen und Systemprivilegien beziehen

#### ➡ Prioritätsklasse

Gibt an wie wichtig der Prozess im Vergleich zu anderen Prozessen ist, gemessen an der zur Ausführung bereitgestellten Prozesszeit.

#### ➡ Begrenzung für Systemressourcen

Speicher- und Ausführungszeitbegrenzung

#### ➡ abgelaufene Ausführungszeit

betriebsbereit seit Prozessstart (ja 3 s Danke ! Rechtschreibreform)

#### ➡ Name

Name der ausgeführten Datei der der Prozess zugeordnet ist

#### ➡ CPU - Nutzung

prozentuale Nutzung des Prozessors in der jüngsten Aktualisierungszeit

#### ➡ Speichernutzung

Größe des Speicherverbrauches in Kb

#### ➡ Seitenfehler

Gesamtzahl von Seitenfehlern die der Prozess seit seines startens erzeugt hat

Was ist ein Seitenfehler ? Klingt schlimmer als es ist. Ein Seitenfehler tritt immer dann auf, wenn vom Prozess benötigte Daten von der Platte in den Arbeitsspeicher übertragen werden müssen.

#### ➡ Größe des virtuellen Speichers

Größe des vom Prozess verwendeten Speichers (Kb) in der Auslagerungsdatei

#### ➡ Basispriorität

Prioritätseinstellungen für den Prozess [niedrig, normal, hoch, Echtzeit]

#### ➡ Auswahl der Handles

gesamte Anzahl der Objekte die vom Prozess geöffnet wurden

## 7.05 Der Schedule Dienst

Dieser Dienst ist für die Verwaltung von Hintergrundprozessen erforderlich. Auf den Schedule Dienst können nur Administratoren zugreifen. Wenn der Dienst nicht gestartet ist, kann er aus der Systemsteuerung/Dienste oder mit `net start schedule` gestartet werden. Nun ist es möglich mit Hilfe des `at`-Befehls Hintergrundprozesse zu verwalten.

#### ➡ `at`

zeigt alle in der Liste stehenden Dienste/Prozesse an

#### ➡ `at [//computer] Zeit Befehl`

[//computer]: Name des Rechners auf dem der Prozess ausgeführt werden soll (optional)

Zeit: gibt an zu welcher Zeit ein Befehl ausgeführt werden soll z.B. 16:00, 4:00 pm, 4pm

#### ➡ `/next:Datum`

legt fest, dass der Befehl am nächsten der angegebenen Tage ausgeführt wird. Mehrere Angaben werden durch Komma getrennt. Es können Wochen- und Monatstage enthalten sein, ohne Datumsangabe wird der aktuelle Tag verwendet.

[`at /next:montag, 23 Befehl`] - am nächsten Montag und am nächsten 23. wird der Befehl ausgeführt

#### ➡ `/every:Datum`

gibt an, dass der Befehl immer wieder ausgeführt werden soll

[`at /every:montag Befehl`] - jeden Montag

#### ➡ `at [//computer] id /delete`

entfernen den Eintrag mit der angegebenen ID

#### ➡ `at [//computer] /delete [/yes]`

entfernt alle Einträge aus der Scheduleliste, /yes ohne Rückfrage

[`at /delete /yes`] - alle Einträge auf der lokalen Maschine werden gelöscht

## Hinweise:

Geplante Aufträge können nicht geändert sondern nur gelöscht werden.

In *at*-Kommandos können nur externe Befehle ausgeführt werden [interne/externe Befehle siehe Grundlagen DOS]. Das Ausführen von internen Befehlen ist aber mit Hilfe von Batchdateien oder *cmd*-Befehl möglich.

*cmd*-Syntax: *cmd /c* Zeichenfolge (Befehl)

## 8. Dateisystem und Festplattenverwaltung

### 8.01 Grundlegende Aufgaben

- ➡ Dateien und Verzeichnisse müssen lokalen- und Domänenbenutzern zugänglich gemacht werden
- ➡ Überwachen und Verwalten des Plattenspeichers
- ➡ Gewährleistung der Dateisystemsicherheit dies sind Schutzsysteme gegen Dateierstörung, Benutzerfehler, Hardwarefehler, usw.
- ➡ Sicherstellen der Vertraulichkeit der Daten, d.h. Regulierung der Rechte
- ➡ Probleme des Dateisystems erkennen und beheben
- ➡ Massenspeicher hinzufügen

### 8.02 Festplatte Benutzern zur Verfügung stellen

- ➡ Partitionieren der Platte
- ➡ Dateisystem erstellen
- ➡ Daten und Verzeichnisse kopieren
- ➡ Zugriff auf das Dateisystem über das Netzwerk ermöglichen

### 8.03 Festplattenstandards

#### 8.031 IDE

- ➡ Integrated Device Equipment, Integrated Device Electronics, Intelligent Drive Electronics (erstgenanntes habe ich am häufigsten gelesen)
- ➡ ein IDE controller besitzt 2 I/O - Kanäle
- ➡ maximal 2 IDE Geräte können an einem Kanal betrieben werden (master, slave)

Auch AT-Bus Festplatte genannt. IDE wurde von Compaq und Western Digital 1984 als Schnittstellen-Standard (40polig) vorgestellt und soll dazu dienen, Diskettenlaufwerke und Festplatten mit möglichst geringem Aufwand anzuschließen. Der vereinfachte Anschluss wurde möglich durch Integration der Steuerelektronik in das Laufwerk. Das erste Gerät mit IDE-Bus erschien 1989.

IDE-Festplatten arbeiten mit 16 Bit und einer Taktfrequenz von 8 MHz. Ihre maximale Kapazität ist auf 528 Megabyte beschränkt. Die Datenübertragungsrate liegt bei 2 MByte/s. Inzwischen gilt der eigentliche IDE-Standard als veraltet. In neueren PCs wird fast nur noch seine Weiterentwicklung EIDE eingesetzt.

## 8.032 EIDE

### ➡ Enhanced Integrated Device Equipment

EIDE ist ein Schnittstellen-Standard, der gegenüber seines Vorgängers IDE vom Festplattenhersteller Western Digital weiterentwickelt wurde und als Antwort auf die Ausbreitung von SCSI gilt. Andere Festplattenhersteller zogen mit ähnlichen Entwicklungen wie "Advanced IDE" (Quantum), "Fast-IDE" oder "Fast-ATA" (beides von Seagate) nach.

EIDE verwendet zwei getrennte Übertragungskanäle und erreicht durch veränderte Transfer- und Adressierungsmethoden eine hohe Datenübertragungsrate. Es können parallel bis zu vier Geräte angesteuert werden. Die EIDE-Schnittstelle unterstützt VL- (Vesa Local) und PCI- (Peripheral Component Interconnect) Bussysteme und ist abwärtskompatibel zu herkömmlichen IDE-Platten.

Im Laufe der Zeit, seit es EIDE gibt, haben sich die Festplatten-Hersteller auf verschiedene Betriebsarten geeinigt. Dadurch wurde es möglich ältere Festplatten parallel zu neueren zu betreiben. Das hatte jedoch den Nachteil, dass die schnellere Festplatte sich der langsameren in ihrer Geschwindigkeit anpassen musste.

Etwas später wurde der Ultra-DMA-Modus (Ultra-ATA) entwickelt. Er unterstützt höhere Datenübertragungsraten und besitzt eingebaute Sicherheitsmechanismen. Die hohe Belastung der CPU bei der Datenübertragung wird durch einen Bus-Master-Treiber reduziert.

Zusammenfassung einiger EIDE-Standards:

Modus	max. Übertragungsrate (theoretisch)
IDE (ATA) PIO 0	3,33 MByte/sek.
IDE (ATA) PIO 1	5,22 MByte/sek.
IDE (ATA) PIO 2	8,33 MByte/sek.
E-IDE (Fast ATA-2) PIO 3	11,11 MByte/sek.
E-IDE (Fast ATA-2) PIO 4	16,66 MByte/sek.
Ultra-DMA/16 (Ultra-ATA) UDMA 0	16,66 MByte/sek.
Ultra-DMA/25 (Ultra-ATA) UDMA 1	25,0 MByte/sek.
Ultra-DMA/33 (Ultra-ATA) UDMA 2	33,33 MByte/sek.
Ultra-DMA/44 (Ultra-ATA) UDMA 3	44,4 MByte/sek.
Ultra-DMA/66 (Ultra-ATA) UDMA 4	66,66 MByte/sek.
Ultra-DMA/100 (Ultra-ATA) UDMA 5	99,99 MByte/sek.
Ultra-DMA/133 (Ultra-ATA) UDMA 6	133 MByte/sek.

### 8.033 SCSI

➔ Small Computer System Interface

➔ abhängig vom Standard bis zu 15 Geräte

➔ jedem Gerät muss eine eindeutige SCSI ID zugewiesen werden

➔ SCSI ist ein Bussystem

➔ Bussysteme müssen beidseitig terminiert werden, somit muss die erste und die letzte SCSI Komponente mit einem Terminator versehen werden. Externe Geräte haben meist einen Autoterminator eingebaut.

#### SE Single Ended

➔ 8 Bit 50-poliger Anschluss für interne Festplatten, CD-ROM- und Band-Laufwerke, SCSI1/2 FAST, max. 7 Geräte, Pfosten-Stecker zweireihig (2x25)

#### SE Centronics Single Ended

➔ 8 Bit 50-poliger Anschluss für externe Festplatten, CD-ROM- und Band-Laufwerke, SCSI1/2 FAST, max. 7 Geräte, Centronics-Stecker (ähnlich Druckerschnittstelle)

#### SE HD50 Single Ended

➔ 8 Bit 50-poliger Anschluss für externe Festplatten, CD-ROM- und Band-Laufwerke, SCSI1/2 FAST, max. 7 Geräte, High-Density-Stecker

#### FW, HD68 Fast Wide

➔ 16 Bit 68-poliger Anschluss für interne und externe Festplatten, CD-ROM- und Band-Laufwerke, max. 15 Geräte, High-Density-Stecker, gleicher Stecker wie FWD jedoch inkompatibel

#### FWD, HD68 Fast Wide Differential

➔ 16 Bit 68-poliger Anschluss für interne und externe Festplatten, CD-ROM- und Band-Laufwerke, max. 15 Geräte, High-Density-Stecker, größere Leitungslänge wie FW, gleicher Stecker wie FW jedoch inkompatibel

#### WC Fast Wide

➔ 16 Bit 80-poliger Anschluss (SCA) für interne Festplatten

Zusammenfassung einiger SCSI-Standards:

SCSI Bezeichnung	max. Übertragungsrate	Datenleitungen	max. Kabellänge	max. Geräte
	(theoretisch)			
SCSI 1	5 MByte/s	8	6 m	7
SCSI 2	5 MByte/s	8	6 m	7
Fast SCSI	10 MByte/s	8	3 m	7
Wide SCSI	20 MByte/s	16	6 m	15
Ultra SCSI	20 MByte/s	8	1,5 m	7
Ultra Wide SCSI	40 MByte/s	16	1,5 m	15
Ultra2 Wide SCSI	80 MByte/s	16	12 m	15
Ultra 160 SCSI	160 MByte/s	16	12 m	15
Ultra 320 SCSI	320 MByte/s	16	12 m	15

## Terminatoren

### ➡ passive Terminatoren

bestehen aus Widerständen

Einsatz bei geringer Anzahl von SCSI-Komponenten und damit auch geringen Spannungsschwankungen auf dem Bus

### ➡ aktive Terminatoren

enthalten Spannungsregler die die Busspannung innerhalb der geforderten Grenzen hält

der SCSI Standard fordert aktive Terminatoren

### ➡ Forced Perfect Terminatoren (FPT)

aktive Terminatoren die mit einer Referenzspannung arbeiten

präzises konstanthalten der Busspannung

FPT - Terminatoren beheben jede Störung auf dem Bus

## Differential SCSI

Es werden für jedes Signal zwei Leitungen zur Verfügung gestellt. Eine Leitung wird mit positiver, die andere mit gleich großer negativer Spannung betrieben. Die eigentliche Information entspricht dem Differenzsignal. Spezielle Kabel, Terminatoren und Controller sind erforderlich.

## 8.04 Übersicht Dateisysteme

Ein Datenträger steht einem Benutzer erst dann zur Verfügung, wenn er ein Dateisystem enthält. Das erstellen des Dateisystems erfolgt üblicherweise durch formatieren des Datenträgers. Bei CD-ROM, RW, DVD usw. wird das Dateisystem beim brennen erstellt.

NT 4.0 unterstützt folgende Dateisysteme:

### ➡ NTFS - NT File System

### ➡ FAT 16 - File Allocation Table

### ➡ ISO 9660 - CD Filesystem

### ➡ Joliet - CD Filesystem

### ➡ ältere NT Versionen z.B. 3.51 unterstützten noch HPFS - High Performance File System - standard OS/2 Dateisystem

## FAT

Entwickelt für DOS/Windows Systeme, NT 4 unterstützt nur FAT 16 kein FAT 32.

## CD - Filesysteme

### ➡ ISO 9660

8.3 Format der Dateinamen; nur Grossbuchstaben (A-Z); Ziffern (0-9)

der Punkt (.) ist erforderlich, auch wenn kein Suffix folgt

Verzeichnisnamen haben kein Suffix

### ➡ Joliet

unterstützt lange Dateinamen (bis 255 Zeichen)

## 8.05 NTFS

NT eigenes Dateisystem. Es kommen Techniken zum Einsatz die die Integrität der Datenstrukturen gewährleisten. Bevor eine Änderung an den Datenstrukturen vollzogen wird, wird die Änderung in einer speziell zu diesem Zweck vorhandenen Protokolldatei festgehalten. Beim Systemstart wird diese Protokolldatei automatisch mit den Strukturen des Dateisystems abgeglichen.

### Dateisicherheit

NTFS-Dateisysteme unterstützen eine als DAC [Discretionary Access Control] bezeichnete Zugriffssteuerung. Diese ermöglicht eine detailliert kontrollierte Zugriffssteuerung.

### verzögertes Schreiben

Schreibvorgänge auf der Festplatte werden nicht sofort ausgeführt, sondern finden zunächst im cache statt. Im Allgemeinen steigert dies zwar die Performance, erhöht aber das Risiko des Datenverlustes.

In einem NTFS befinden sich Zeiger für alle Dateien und Verzeichnisse als Einträge in der MFT [Master File Table]. Die Information über die Struktur des Dateisystems, sogenannte Metadaten werden in den ersten 16 Einträgen der MFT gespeichert.

### Metadateien

Datei	Inhalt
\$	Hauptverzeichnis des Dateisystems
\$MFT	Inhalt der MFT
\$MFT MIRR	Speicherort der Kopie der Metadateien
\$LOGFILE	Protokoll
\$VOLUME	Datenträgerinformation einschliesslich Name der NTFS Version
\$ATTRDEF	Definitionstabelle der Attribute
\$BITMAP	Abbilddatei die den Status jedes Clusters im Dateisystem kennzeichnet
\$BOOT	Startdatei
\$BADCLUS	Liste der defekten cluster
\$QUOTA	reserviert um den Plattenplatz für Benutzer begrenzen zu können

### Verwaltung von Dateien unter NTFS

Eine Datei stellt eine Sammlung von Eigenschaften dar.

mögliche Eigenschaften:

- ➡ DOS Attribute
- ➡ Zeitstempel
- ➡ Anzahl der hard links [mit Hilfe von hard links kann eine Datei mehrere Dateinamen erhalten]

### Dateiname

- ➡ maximal 255 Zeichen
- ➡ alle Zeichen und Symbole sind erlaubt - Ausnahmen: ? " \ / \* : < > |

## Sicherheitsmerkmale

- ➔ Zugriffsberechtigungen unter NT
- ➔ Indexdaten für Verzeichnisse
- ➔ Datenattribute [Dateiinhalte]

## 8.06 Formatieren und Verwalten des Dateisystems

Es gibt unter NT zwei Möglichkeiten ein Dateisystem zu erstellen:

- ➔ Festplattenmanager (grafisch)
- ➔ `format`-Befehl in der Eingabeaufforderung

### **format-Befehl**

Syntax:

- ➔ `format [/fs: Dateisystem] Laufwerksbuchstabe`
- ➔ `format [/v: Bezeichnung] Laufwerksbuchstabe`
- ➔ `format [/c][/a:n] Laufwerksbuchstabe`

*/fs: Dateisystem*

- ➔ bestimmt das Dateisystem
- ➔ NTFS oder FAT
- ➔ standardmäßig wird der Typ eines vorhandenen Dateisystems übernommen
- ➔ eine leere Partition wird als FAT formatiert

*/v: Bezeichnung*

- ➔ bestimmt die Datenträgerbezeichnung

*/c:*

- ➔ aktiviert die automatische Komprimierung

*/a:n*

- ➔ bestimmt die Größe einer Zuordnungseinheit oder Cluster (Einheit, mit der Platz innerhalb des Dateisystems belegt wird)

Vorgaben:

Zuordnungseinheit	Dateisystem
512 Byte	bis 512 MByte
1 kByte	> 512 MByte bis 1 GByte
2 kByte	> 1 GByte bis 2 GByte
4 kByte	> 2 GByte

erlaubte Größen: 512 Byte bis 64kByte (in 2er Potenzen)

## Dateikomprimierung

NTFS-Dateisysteme beherrschen die automatische Komprimierung. Seitens des Benutzers sind keine weiteren Maßnahmen erforderlich. Komprimierung erfolgt mittels des Befehls `compact`.

Syntax: `compact [/c] [/u] [Optionen] [Datei]`

`/c` bzw. `/u`

➡ bestimmen ob die angegebenen Elemente komprimiert `[/c]` oder dekomprimiert `[/u]` werden sollen

➡ ohne diese Angaben wird der Zustand der angegebenen Elemente angezeigt

## Dateisystem aufsetzen bzw. mounten

Alle lokalen Dateisysteme werden beim Systemstart automatisch aufgesetzt. Mit Hilfe von `chkdsk` kann die Konsistenz eines Dateisystems geprüft werden. Fehler werden angezeigt und können üblicherweise behoben werden. Reparaturen sind zumeist mit keinem oder nur geringem Datenverlust verbunden. `Chkdsk` wird automatisch beim Systemstart ausgeführt, wenn das Dateisystem nicht ordnungsgemäß abgesetzt wurde.

## Konvertieren von FAT Dateisystemen

`convert /fs:NTFS Laufwerksbuchstabe`

## 8.07 NTFS-Dateisystem erweitern

Datenträger die durch einen eindeutigen Laufwerksbuchstaben definiert sind, können mehr als eine Partition umfassen. Werden mehrere Partitionen für ein Dateisystem verwendet, so wird diese Sammlung von Partitionen als Datenträgersatz bezeichnet.

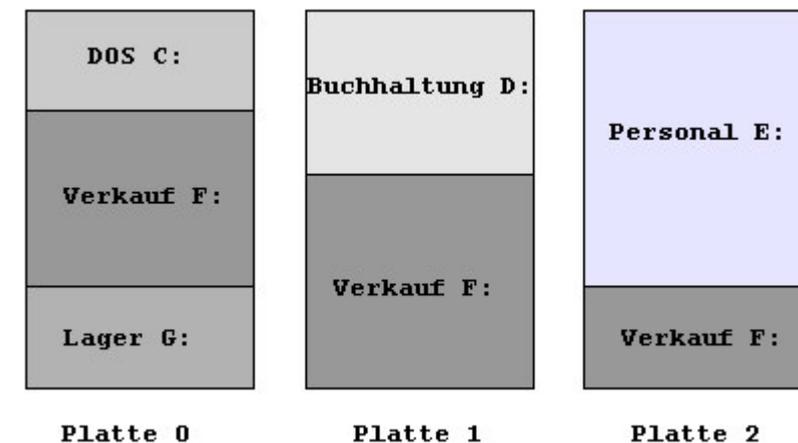


Abbildung IV: Dateisystem über mehrere Partitionen

Wird ein bestehendes Dateisystem erweitert, muss das System neu gestartet werden. Bei diesem Neustart wird automatisch *chkdsk* ausgeführt. Wird ein neuer Datenträgersatz erstellt, so muss darauf ein Dateisystem installiert werden, d.h. er muss formatiert werden. Bei Ausfall einer Komponente wird das ganze Dateisystem unbrauchbar. Wenn ein Datenträgersatz aufgelöst werden soll, müssen alle Daten gesichert werden (wenn man sie noch braucht), sonst gehen sie verloren.

## 9. RAID Systeme

Abkürzung für "Redundant Array of Independent Disks" oder "Redundant Array of Inexpensive Disks". Bei RAID-Systemen steht zunächst die Sicherheit von Festplatten-Daten im Vordergrund. Ein RAID-System ist nämlich in der Lage, Daten - gegebenenfalls redundant - auf mehreren Festplatten abzulegen. RAID-Systeme setzen sich immer aus mehreren Festplatten zusammen. (Der Begriff "RAID - Redundant Array of Inexpensive Disks" soll übrigens 1987 an der Universität von Kalifornien, Berkeley, festgelegt worden sein.)

Im RAID System ist dazu ein Festplatten-Controller notwendig, der über integrierte Management-Funktionen verfügt. Für die Anwendungen und für das Betriebssystem stellt sich das Array (die Batterie einzelner Festplatten) als eine große Festplatte dar; die Daten-Verwaltung - welche Daten werden wo abgelegt? - wird vom System selbst übernommen. Ein Merkmal moderner RAID-Systeme besteht - neben der Sicherheit - zudem darin, dass defekte Platten im laufenden Betrieb ausgetauscht werden können, so dass außer den Netzwerkadministratoren üblicherweise niemand etwas von einem Ausfall merkt.

Es existieren mehrere "RAID-Levels", die über unterschiedliche Leistungsmerkmale verfügen. Die Grundlage der RAID-Technologie wird durch sogenannte "Stripe Sets" gebildet (stripe = Streifen). Dabei werden relativ kleine Datenblöcke - im Bereich von einigen KByte - auf mehrere Festplatten verteilt. Ursprünglich wurden die RAID-Levels 1 bis 5 definiert. Mitte der 90er Jahre sind noch die Levels 6 und 7 hinzugekommen. Allerdings kann vom Zahlenwert eines Levels nicht direkt auf die Qualität oder auf die Funktionalität des entsprechenden RAID-Systems geschlossen werden. Es handelt sich lediglich um eine von Professoren der Universität Berkeley ziemlich willkürlich gewählte Art der Bezeichnungsfindung. Da aber selbst diese Untergliederung noch nicht ausreicht, um sämtliche Leistungsmerkmale von RAID-Systemen zu spezifizieren, werden auch Kombinationen dieser Benennungen verwendet.

### **RAID 0**

Der RAID-Level 0 wird auch als "Non-Redundant Striped Array" bezeichnet. Die "0" steht also für "keine Redundanz" bzw. "keine Sicherheit". Im RAID-0-System werden zwei und mehr Festplatten zusammengeschaltet, um die Schreib-Lese-Geschwindigkeit zu erhöhen - z.B. zur Verarbeitung von digitalen Video-Daten. Die beim Benutzer entstehenden Daten werden in kleine Blöcke mit einer Größe von 4 bis 128 KByte aufgeteilt. Diese Blöcke werden abwechselnd auf den Platten des RAID-0-Arrays gespeichert. So kann auf mehrere Platten gleichzeitig zugegriffen werden, was die Geschwindigkeit insbesondere bei sequentiellen Zugriffen erhöht. Da bei RAID 0 keine redundanten Informationen erzeugt werden, gehen Daten verloren, wenn eine RAID-Platte ausfällt. Und da die Daten einer Datei auf mehrere Platten verteilt sind, lassen sich auch keine zusammenhängenden Datensätze mehr reproduzieren, selbst wenn nur eine Platte im RAID-0-Array ausfällt. 2 Platten mit je 100 GB im Raid 0 bedeutet, man hat ein 200 GB Array was wesentlich schneller ist wie eine einzelne Platte.

## **RAID 1**

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.

## **RAID 2**

Das RAID 2-System teilt die Daten in einzelne Bytes auf und verteilt sie auf die Platten des Platten-Arrays. Der Fehlerkorrekturcode (ECC = Error Correction Code) wird nach dem Hamming-Algorithmus berechnet und auf einer zusätzlichen Platte gespeichert. Da in allen modernen Festplatten bereits Methoden zur Fehlerkorrektur enthalten sind, spielt dieser RAID-Level in der Praxis keine große Rolle mehr.

## **RAID 3**

In einer RAID-3-Konfiguration werden die Daten in einzelne Bytes aufgeteilt und dann abwechselnd auf den - meistens zwei bis vier - Festplatten des Systems abgelegt. Für jede Datenreihe wird ein Parity-Byte hinzugefügt und auf einer zusätzlichen Platte - dem "Parity-Laufwerk" - abgelegt. Beim Ausfall einer einzelnen Festplatte können die verlorengegangenen Daten aus den verbliebenen sowie den Parity-Daten rekonstruiert werden. Da moderne Festplatten und Betriebssysteme aber nicht mehr mit einzelnen Bytes arbeiten, findet auch der RAID-Level 3 kaum noch Verwendung.

## **RAID 4**

Prinzipiell ist RAID 4 mit RAID 3 vergleichbar. Nur werden die Daten nicht in einzelne Bytes, sondern in Blöcke von 8, 16, 64 oder 128 KByte aufgeteilt. Beim Schreiben von großen sequentiellen (zusammenhängenden) Datenmengen läßt sich so eine hohe Performance erreichen. Werden verteilte Schreibzugriffe vorgenommen, muss jedesmal auf den Parity-Block zugegriffen werden. Für viele kleine Zugriffe ist RAID 4 demnach nicht geeignet.

## **RAID 5**

Beim RAID-5-Level werden die Parity-Daten - im Unterschied zu Level 4 - auf allen Laufwerke des Arrays verteilt. Dies erhöht die Geschwindigkeit bei verteilten Schreibzugriffen. Engpässe durch die spezielle Parity-Platte können nicht entstehen. Bedingt durch diese Vorteile hat sich RAID 5 in den letzten Jahren beliebteste RAID-Variante für PC-Systeme etabliert.

## **RAID 6**

RAID 6 bietet die höchste Datensicherheit. Dabei wird zum RAID-5-Verfahren eine weitere unabhängige Paritäts-Information auf einem zusätzlichen Laufwerk hinzugefügt. Dadurch werden allerdings die Schreibzugriffe wieder etwas langsamer.

## **RAID 7**

Auch RAID 7 ist ähnlich wie RAID 5 aufgebaut. In der RAID-Steuereinheit wird bei RAID 7 aber zusätzlich ein lokales Echtzeitbetriebssystem eingesetzt. RAID 7 benutzt schnelle Datenbusse und mehrere größere Pufferspeicher. Die Daten in den Pufferspeichern und auf den Laufwerken sind von der Datenübertragung auf dem Bus abgekoppelt (asynchron). So werden alle Vorgänge gegenüber den anderen Verfahren erheblich beschleunigt. Ähnlich wie bei RAID 6 kann die Paritätsinformation für eines oder mehrere Laufwerke generiert werden. Es lassen sich gleichzeitig unterschiedliche RAID-Level nutzen.

## **RAID 10 bzw. RAID 0+1**

Eigentlich handelt es sich bei RAID 10 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 Performance vereinigt. Bei RAID 10 werden üblicherweise vier Festplatten verwendet, denn dieses System verlangt nach zwei Paaren gespiegelter Arrays, die dann zu einem RAID-0-Array zusammengefaßt werden. RAID 10 eignet sich insbesondere zur redundanten Speicherung von großen Dateien. Da hierbei keine Parität berechnet werden muss, sind die Schreibzugriffe mit RAID 10 sehr schnell. RAID 10 gilt übrigens auch als zusätzlich gestrippte Version von RAID 1.

## **RAID 30**

RAID 30 wird eingesetzt, wenn große Dateien sequentiell übertragen werden sollen. Es handelt sich um eine zusätzlich gestrippte Version von RAID 3. Diese Version wurde von AMI (American Megatrends) entwickelt. Sie bietet Datensicherheit und sehr hohen Durchsatz. RAID 30 ist komplexer als niedrigere RAID-Level und benötigt mehr Platten. AMI benutzt RAID 30 mit sechs Festplatten.

## **RAID 50**

Werden sowohl große Datensicherheit wie auch schnelle Zugriffszeiten und hohe Datentransfer-Raten benötigt, empfiehlt sich RAID 50. Auch diese Version stammt von AMI. Sie ist ebenfalls komplexer als niedrigere RAID-Level und benötigt ebenfalls sechs Festplatten. RAID 50 ist die gestrippte Version von RAID 5.

## **andere Kombinationen**

Aus den genannten RAID-Levels lassen sich noch viele weitere Kombinationen ableiten. In der Praxis erstellen sich größere Unternehmen maßgeschneiderte Einzellösungen, die zwar auf einer oder mehreren RAID-Technologien basieren, jedoch nicht direkt in die genannten RAID-Standards eingereiht werden können. Beliebte sind beispielsweise auch die Kombinationen aus RAID 0 und 3 oder aus RAID-Level 3 und 5. Hier beginnt allerdings schon das Bezeichnungschao, denn die Kombination aus 0 und 3 wird mit RAID 53 bezeichnet, und die Kombination aus 3 und 5 nennt sich schließlich RAID 8. Neben den verschiedenen RAID-Levels existieren zusätzlich noch diverse Implementierungen von RAID. Bei Software-RAID-Lösungen beispielsweise wird ein Treiber ins Betriebssystem integriert, der RAID-Funktionalitäten enthält. Praktisch alle modernen Server-Betriebssysteme unterstützen verschiedene RAID-Levels. Allerdings sollte bei einer solchen Lösung zusätzliche Prozessor-Leistung eingeplant werden. ABER ACHTUNG: Ein nicht zum RAID gehörendes Boot-Laufwerk, von dem der spezielle RAID-Treiber geladen werden soll, würde die angestrebte Sicherheit bei einem Ausfall sofort zunichte machen. Ein externes RAID-System (SCSI to SCSI RAID) - eine hardwarebasierende RAID-Lösung - kennt diese Probleme dagegen nicht. Das Betriebssystem kann dabei direkt vom RAID-Controller geladen werden. Hier wird die RAID Funktionalität vom Controller gesteuert. Auch "Zwitterlösungen" sind verfügbar. So werden bei der AAA- oder bei der ARO-Serie von Adaptec RAID-Treiber auf dem Server eingesetzt, während die Berechnung der Redundanz-Informationen (Parität) auf einen Coprozessor auf dem RAID-Hostadapter ausgelagert ist. Echte Hardware-RAID-Controller können (meist über SCSI an den Server angebunden) in einem eigenen Gehäuse untergebracht sein, was allerdings eine relativ teure Lösung ist. Im PC Server-Bereich finden sich meist Host-basierende RAID-Lösungen, wobei der Controller direkt in den Server eingesteckt wird. Damit sind sehr hohe Transferraten möglich, und die Konfiguration ist äußerst flexibel.

ÜBRIGENS: Nicht nur dann, wenn das RAID System zur Erhöhung der Datensicherheit eingesetzt wird, empfiehlt sich der Einsatz einer unterbrechungsfreien Stromversorgung (USV).

## 10. Copyleft, Quellen, Credits, Versionen

### 10.01 Copyleft (c) 2002 ST.

Es wird die Erlaubnis gegeben dieses Dokument zu kopieren, verteilen und/oder zu verändern unter den Bedingungen der GNU Free Documentation License, Version 1.1 oder einer späteren, von der Free Software Foundation veröffentlichten Version. Eine Kopie dieser Lizenz ist im Netz unter <http://www.gnu.org/copyleft/fdl.html> zu finden.

Eine deutschsprachige Version gibt es hier:  
<http://nautix.sourceforge.net/docs/fdl.de.html>

Der Begriff copyleft ist ein neuer, von GNU eingeführter Begriff. Es ist ein Wortspiel eines englischen Wortes, das aus "copyright" "copyleft" macht, und damit ausdrückt dass es kopieren nicht verbietet, sondern erlaubt unbeschränkt unter vertraglichen Bedingungen zu kopieren.  
<http://www.gnu.org/copyleft/copyleft.de.html>

Dieses Script gibt es als html- und pdf- Version sowie die Quelldatei als StarOffice Dokument im Netz unter: <http://st23.de>

### 10.02 Quellen

Grundstudium Informatik [2002] 2.Semester "Betriebssysteme #2 - Windows NT"  
Vorlesungen + Praktika an der Naturwissenschaftlich Technischen Akademie Isny.  
<http://www.fh-isny.de/>

[Ass. Schäfer, Dipl. Inf. Steinemann]

Windows NT 4.0-Taschenbuch [ISBN 3-89360-930-X]

[Eric Dornwaß, Patrick Schleicher]

<http://www.glossar.de/>, <http://www.computer-woerterbuch.de/>

<http://www.e-online.de/>, <http://www.google.de/>

### 10.03 Credits

Vielen Dank an Slide für das zur Verfügung stellen des NT-Taschenbuches und ihrer NT-Workstation.

Dank auch an Caro und Sandra für ihre Aufzeichnungen.

### 10.04 Versionsänderungen

1.01	erste öffentliche Version
1.02	GNU Free Documentation License wurde integriert
1.10	Erweiterung des Punktes 8.07 NTFS Dateisystem erweitern Kapitel 9 RAID Systeme hinzugefügt Punkt 10.04 Versionsänderungen hinzugefügt Ergänzungen und Rechtschreibkorrekturen auf allen Seiten

Für Hinweise, Kritik und Fehlermeldungen bin ich jederzeit dankbar.

Ansonsten, viel Erfolg und Spass am Gerät ;-) ...

[STephan]  
st@st23.de