# Zusammenfassung aus den Kursunterlagen

## MOC 70-210 und 70-215 für Windows 2000 Professional und Server



## <u>Inhaltsverzeichnis</u>

Unterrichtseinheit 1	Seite
Windows 2000 Arten	1
Systemanforderungen	1
Lizenzierungsmodus	1
Domäne oder Arbeitsgruppe	2
Erforderliche Benutzer - und Computerkonten zum Domänenbeitritt	2
Installationsdisketten erstellen	2
W2K Server nachträglich konfigurieren	2
Aktualisieren von Windows 2000	2
Generieren eines Kompatibilitätsberichts	3
Aktualisieren auf Windows 2000 Advanced Server	3
Sichern wichtiger Datendateien und Einstellungen vor der Aktualisierung	4
Unterrichtseinheit 2	Seite
Installieren von Hardware unter Windows 2000	1
Aktualisieren von Treibern	1
Verwalten der Treibersignierung Konfiguration der	1
Treibersignierungsoptionen	1
Ermitteln unsignierter Dateien	1
Hardwareprofile	1
Erstellen eines Hardwareprofils Konfigurieren der Anzeigeoptio- nen	1
•	2
. termiganoren momeron momero	

	Konfigurieren von Systemeinstellungen	2
	Reihenfolge der Umgebungsvariablen	3
	Ändern von Start- Wiederherstellungsoptionen	3
	Konfigurieren der Desktopum- gebung	4
	Konfigurieren der Ländereinstellung	4
	Konfigurieren von Eingabehilfen	4
	Verwalten von Anwendungen	4
	Konfigurieren von Internetoptionen für Clientcomputer	5
Unterrichts	seinheit 3	Seite
	Netzwerke unter Windows 2000	1
	Herstellen einer Verbindung zu einem Microsoft Netzwerk	1
	Vergeben einer statischen IP- Adresse	2
	Überprüfen und Testen einer TCP/IP Konfiguration	2
	Herstellen einer Verbindung zu einer Netzwerkressource unter W2K	3
	Herstellen einer Verbindung zu einem Novell Netware-Netzwerk	3
	Installation und Konfiguration von NWLink	3
	Konfiguration eines Rahmen - typs	4
	Kofiguration einer Netzwerk-	4

Herstellen einer Verbindung zu
einer Netware Netzwerk-
ressource

## Seite

.....4

Erstellen und Verwalten von Benutzerkonten	1
Lokale Benutzerkonten	1
Domänenbenutzerkonten	1
Vordefinierte Benutzerkonten	1
Namenskonventionen	1
Kennwortrichtlinien	2
Kontooptionen	2
Erstellen eines lokalen Benutzerkontos	2
Verwaltungsprogramme von Windows 2000	2
Verwalten von Benutzerdaten durch das Erstellen von Basis- ordnern	3
Eigenschaften für Domänenbe- nutzerkonten	4
Anmeldezeiten für Domänen- benutzerkonten	4
Erstellen von Benutzerkonten	5
Erstellen eines servergespei- cherten Profils	6
Erstellen eines verbindlichen servergespeicherten Profils	6
Optimale Methoden für das Erstellen und Verwalten von Benutzerprofilen	7

## Seite

Arbeitsweise von Windows Gruppen	2000 <b>1</b>
Gruppen in einer Arbeitsgru	ppe1
Gruppen in einer Domäne	1
Lokale Gruppen	1
Integrierte lokale Gruppen	2
Strategie zum Verwenden v lokalen Gruppen in einer Arbeitsgruppe (ALP-Strateg	
Erstellen von lokalen Grupp	en2
Implementieren von Gruppe einer Domäne	en in2
Gruppentypen	3
Gruppenbereiche	3
Integrierte und vordefinierte Gruppen in einer Domäne	4
Gruppen in einer Domäne (AGDLP-Strategie)	4
Richtlinien für das Erstellen Domänengruppen	von4
Erstellen und Löschen von Domänengruppen	4
Hinzufügen von Domänenm gliedern zu Domänengrupp	
Unterrichtseinheit 6	Seite
NTFS Berechtigungen	1
NTFS Ordnerberechtigunge	en1
NTFS Dateiberechtigungen	2

	Mehrfache NTFS-Berechtigungen	2
	Vererbung von NTFS- Berechtigungen	2
	Erteilen von NTFS-Berechtigungen	3
	Optimale Methoden zum Erteilen von NTFS-Berech- tigungen	3
	Erteilen spezieller NTFS- Berechtigungen	3
	Komprimieren von Daten auf einer NTFS-Partition	4
	Festlegen des Komprimierungs- status	4
	Kopieren und Verschieben von komprimierten Dateien und Ordnern	4
	Optimale Methoden zum Komprimieren von Daten	5
	Konfigurieren von Datenträgerkontigenten auf NTFS-Partitionen	5
	Verschlüsseln eines Ordners oder einer Datei	6
	Wiederherstellen eines ver- schlüsselten Ordners oder Datei	6
Unterrichts	seinheit 7	Seite
	Freigegebene Ordner	1
	Erstellen freigegebener Ordner	1
	Anforderung für das Freigeben von Ordnern	1
	Freigeben eines Ordners	1
	Berechtigungen	2

	Mehrfaches Freigeben eines Ordners	3
	Herstellen einer Verbindung zu einem freigegebenen Ordner	3
	Kombinieren von NTFS- Berechtigungen und Berechti- gungen für freigegebene Ordner	3
	Verwenden von administrativen freigegebenen Ordnern	4
	Veröffentlichen eines freigege- benen Ordners in Active Directory	4
	Einführung in DFS (Distributed File System)	4
	Arten von DFS-Stämmen	5
	Zugreifen auf Dateiressourcen über DFS	5
	Erstellen eines DFS-Stammes	6
	Hinzufügen von DFS-Ver- knüpfungen	6
	Replikate für die Fehlertoleranz	6
	Konfigurieren der Replikation	6
Unterrichts	seinheit 8	Seite
	Uberwachen von Ereignisproto- kollen	1
	Einführung in Ereignisprotokolle	1
	Anzeigen von Ereignisproto- kollen	2
	Verwalten von Ereignisproto- kollen	2
	Verwenden des Task-Managers	3
	Anzeigen der Leistungsindi- katoren	4
	Verwenden von Warnungen	4

	Optimieren der Leistung	5
	Untersuchen der Arbeitsspei- cherleistung	5
	Untersuchen der Prozessor- leistung	6
	Untersuchen der Netzwerkleistung	7
Unterrichts	seinheit 9	Seite
	Verschiedene Arten von Richtlinien	1
	Implementieren von Sicherheit auf mehreren Computern	1
	Verwenden von vordefinierten Sicherheitsvorlagen	3
	Überwachung des Zugriffs auf Systemressourcen	4
	Planen einer Überwachungsrichtlinie	5
Unterrichts	seinheit 10	Seite
	Begriffe zum Drucken unter	
	W2K	1
	Anforderungen für das Konfigurieren eines Netzwerkdruckers	1
	Anforderungen für das Konfigurieren eines Netzwerk-	
	Anforderungen für das Konfigurieren eines Netzwerkdruckers Hinzufügen und Freigeben eines Druckers für ein lokales	1
	Anforderungen für das Konfigurieren eines Netzwerkdruckers  Hinzufügen und Freigeben eines Druckers für ein lokales Druckgerätes  Hinzufügen und Freigeben eines Druckers für ein Netz-werk	1
	Anforderungen für das Konfigurieren eines Netzwerkdruckers  Hinzufügen und Freigeben eines Druckers für ein lokales Druckgerätes  Hinzufügen und Freigeben eines Druckers für ein Netz-werk Druckgerät  Verwenden des Assistenten zum Hinzufügen eines Standard TCP-IP Druckerports	2

	Konfigurieren eines Netzwerk- druckers	4
	Erstellung eines Druckerpools	5
	Festlegen von Druckeroptionen	5
	Zuweisen von Druckerberechtigungen	5
	Kontigurieren des Internet- druckens	7
	Einrichten des Internetdruckens mit Hilfe eines Webbrowsers	7
Unterricht	seinheit 11	Seite
	Konfigurieren der Hardware für die mobile Datenverarbeitung	1
	Erstellen eines Hardwareprofils für mobile Benutzer	1
	Verwenden von Dockingstatio- nen	1
	Konfigurieren der Energiever- waltungsoptionen für mobile Datenverarbeitung	2
	Verwenden von Energiespar- optionen	2
	Dateien offline verfügbar machen	3
	Konfigurieren eines Servers für Offlinedateien	3
	Konfigurieren eines Clients für Offlinedateien	4
	Verwenden der Synchronisationsverwaltung zum Synchronisieren von	4
	Herstellen von Verbindungen zu Netzwerken und Computern	4
	Herstellen von Verbindungen zu einem privaten Netzwerk über das Internet	5

## Seite

## **Unterrichtseinheit 12**

Festplattentypen unter W2K	1
Basisfestplatten	1
Dynamische Festplatten	1
Erstellen von Partitionen auf einer Basisfestplatte	2
Erstellen von Datenträgern auf einer dynamischen Festplatte	2
Aktualisieren von einer Basis- festplatte auf eine dynamische Festplatte	2
Aktualisierungsergebnisse	3
Erstellen von einfachen Datenträgern	4
Erweitern einfacher Daten-träger	4
Reparieren von Partitionen und Datenträgern	4
Löschen von Partitionen und Datenträgern	4
Hinzufügen von Festplatten von anderer Computer	5
Importieren unvollständiger Datenträger	5
Verwalten von Laufwerks- buchstaben	5
Verwalten von Laufwerkpfaden	5
Remoteverwaltung von Fest- platten	6
Defragmentierung von Partitionen	6

Konfigurieren einer USV	1
Implementieren von Fehlertole- ranz mit Hilfe von RAID	1
Softwareimplementierung von RAID Harwdwareimplementierung von RAID	1
Gespiegelte Datenträger	2
RAID 5 Datenträger	3
Vorteile von RAID5 Datenträger	3
Nachteile von RAID5 Daten- träger	3
Wiederherstellen eines fehler- haft gespiegelten Datenträgers auf einer Festplatte	3
Ersetzen einer Festplatte und Erstellen eines neuen gespie- gelten Datenträgers	4
Wiederherstellen eines fehler- haft RAID5 Datenträgers auf einer Festplatte	4
Ersetzen einer Festplatte und Erstellen eines neuen RAID 5 - Datenträgers	4
Übersicht über Datensicherung und Wiederherstellung	4
Berechtigungen und Benutzer- rechte zum Sichern	5
Sicherungsarten	5
Sichern der Systemstatus-daten	5
Verwenden der Wiederher- stellungstools für Notfälle	6

	Wiederherstellen eines Computers mit Hilfe der Wiederherstellungskonsole	7
	Wiederherstellen eines Computers mit Hilfe des Notfall- reparaturvorgangs	7
Unterrichts	seinheit 14	Seite
	Einführung in die Terminaldienste	1
	Funktionsweise der Terminal- dienste	1
	Benutzerumgebungen	1
	Features und Vorteile	1
	Zentralisierte Bereitstellung von Spartenanwendungen	2
	Zugriff auf den W2K Desktop	2
	Erweiterte Support- und Verwaltungsmöglichkeiten	2
	Identifizieren der Clientan- wendungen	2
	Windows basierte Anwendungen	2
	MS DOS Anwendungen	3
	Bestimmen der Serverkonfiguration	3
	Benutzereigenschaften	4
	Identifizieren der Lizenzierungs- anforderungen	4
	Richtlinien für einen Lizenzserver	4
	Arten von Clientlizenzen	5
	Installieren der Terminaldienste	5
	Konfigurieren des Benutzerzugriffs	6

Erstellen disketten	von Clientinstallations-	6
	den der Clientsoftware Netzwerk	6
	n einer Verbindung zu erminalserver	6
Beenden	einer Terminalsitzung	6
	on von Anwendungen n Terminalserver	7
Unterrichtseinheit	15	Seite
Bereitstel	llen von W2K	1
Durchfüh Installatio	ren einer manuellen on	1
	n von Installationen und erungen mit Hilfe von n	2
	es Installationspro- Winnt.exe mit Hilfe von	2
	es 32-Bit-Installations- ns Winnt32.exe mit	3
Verwende und UDF	en von Antwortdateien -Dateien	3
	es Assistenten für den onsmanager	4
Angeben variatione	eindeutiger Computer- en	4
Verwende duplizieru	en der Festplatten- ung	5
	hen des Vorgangs der enduplizierung	5
reitungsp SYSPRE	rogramms P.EXE	6
Installiere von RIS	en von W2K mit Hilfe	6
	eren von Clients für die nstallation	6

## Seite

Implementiren von Windows 2000 basierten Servern	1
Verfügbare Serverfunktionen	1
Lastenausgleich	1
Dokumentieren der Supporttätigkeiten	1
Allgemeine Implementierungsschritte	2
Implementieren eines Dateiservers	2
Vorbereiten der Festplatten für Dateiserver	2
Vorbereiten der Festplatten für Druckserver	2
Konfigurieren von Druckerfreigaben und Druckerrechten	3
Vorbereiten der Festplatten für Anwendungsserver	3

#### Windows2000-Arten:

- Windows2000-Professional (Nachfolger von NT-Workstation) unterstützt bis zu 2 Prozessoren
- Windows2000-Server (Nachfolger von NT Mitgliedsserver / Memberserver)
   (Diese Version eignet sich ideal für Datei-, Druck- und Webserver, da sie Terminaldienste einschließt) unterstützt bis zu 4 Prozessoren
- Windows2000-Advanced Server
   (erhöhte Skalierbarkeit; schließt Clustering [Zusammenarbeit mehrerer Server, um
   eine Verfügbarkeit serverbasierter Anwendungen beizubehalten] und Lastenausgleich
   ein) unterstützt bis zu 8 Prozessoren
- Windows2000-Datacenter Server (Unterstützt größeren Speicher und Multi-CPU) unterstützt bis zu 16 Prozessoren

#### Systemanforderungen:

CPU: mindestens P133

Speicherplatz: 2 GB mit mindestens 1 GB freiem Speicherplatz

Arbeitsspeicher: - W2K-Professional: mindestens 64MB

- W2K-Adv.Server: 128MB unterstützt, 256MB empfohlen

Alle unterstützten Geräte von W2K befinden sich in der **Hardwarekompatibilitätsliste** (HCL) auf der **Windows 2000 CD** im **Ordner Support** im **HCL.txt**.

Das Dateiformat von W2K sollte NTFS (Sicherheit auf Datei- und Ordnerebene, Dateikomprimierung, Datenträgerkontingente, Dateiverschlüsselung) sein. Nur bei einer Dualbootkonfiguration empfiehlt es sich FAT32 zu wählen!

**Achtung:** Dateikomprimierung und Dateiverschlüsselung können nie gleichzeitig angewendet werden!

## <u>Lizensierungsmodus:</u>

Bei der Installation von Windows2000 Advanced Server ist eine Clientzugriffslizensierung (CAL, Client Access License) für jeden zugreifenden Clientcomputer (zusätzlich zu dessen Lizenz) notwendig.

Es wird unterschieden zwischen:

- **Pro-Arbeitsplatz-Lizenzierung** (bei mehr als einem Server geeignet) jeder Client kann auf eine beliebige Anzahl Server mit nur einer CAL zugreifen
- **Pro-Server-Lizenzierung** (bei nur einem Server geeignet) jede Client-Verbindung mit dem Server erfordert eine CAL auf dem Server

(Man kann von einer Pro-Server-Lizenz zu einer Pro-Arbeitsplatz-Lizenz wechseln, allerdings nicht umgekehrt)

#### Domäne oder Arbeitsgruppe?

#### Arbeitsgruppe:

- Ressourcen, Verwaltung und Benutzerauthentifizierung werden auf jedem Computer in der Arbeitsgruppe durchgeführt
- Jeder Computer hat eine eigene lokale SAM-Datenbank (Security Accounts Manager); ein Benutzer muß über ein Benutzerkonto auf den zugreifenden Computer besitzen
- Es gibt höchstens 10 Computer

#### Domäne:

- Resourcen, Verwaltung und Benutzerauthenifizierung sind zentralisiert
- Es gibt nur eine SAM-Verzeichnisdatenbank (Active Directory), in der alle Benutzerkonten für die Domäne gespeichert werden; ein Benutzer benötigt nur ein Domänenbenutzerkonto, um auf alle gemeinsam genutzten Netzwerkressourcen in der Domäne zugreifen zu können
- Domänen sind skalierbar (von zwei bis mehreren tausend Computern)

#### **Erforderliche Benutzer- und Computerkonten zum Domänenbeitritt:**

- Es muß ein Benutzerkonto im Active Directory verfügbar sein
- Ein vorhandenes Computerkonto im Active Directory (Name des Computers muß mit Namen im Activ Directory übereinstimmen)
- Standardmäßig kann jedes Domänenbenutzerkonto bis zu 10 Computerkonten erstellen

Um Installationsdisketten für W2K zu erstellen muß man das Programm **Makeboot.exe** (**Windows2000 CD** im **Ordner Bootdisk**) unter einem anderen W2K-Rechner ausführen. (<u>Syntax:</u> Start→Ausführen→makeboot a:→OK)

Um einen W2K-Server nachträglich zu konfigurieren, muß folgendes Durchgeführt werden:

Start→Programme→Verwaltung→Konfiguration des Servers Hier kann folgendes konfiguriert werden:

- Active Directory
- Datei-, Druck- und Web-/Mediaserver
- Netzwerk
- Anwendungsserver
- Weitere erweiterte Konfigurationen (z.B. Message Queueing, W2K Support Tools...)

#### Aktualisieren von W2K:

Windows95 und Windows98  $\rightarrow$  Windows2000 Professional WindowsNT Workstation 3.51/4.0(SP4)  $\rightarrow$  Windows2000 Professional Windows für Workgroups 3.1  $\rightarrow$  WindowsNT Workstation 3.51/4.0  $\rightarrow$  W2K Windows95/98  $\rightarrow$  W2K

(Die Aktualisierung von WinNT zu W2K ist der am meisten empfohlene Aktualisierungsgrad, da hier nur einige unbedeutende Inkompatibiliäten auftreten !!!)

#### Generieren eines Kompatibilitätsberichts:

Um ungewollte Inkompatibilität einiger Anwendungen – vor allem von Windows 95/98 – vorzubeugen, verfügt W2K über einen NUR-Berichtsmodus, welcher Informationen zu inkompatiblen Features und Anwendungen erstellt.

Es gibt zwei Arten, diesen Bericht zu erstellen:

- 1) Start→Ausführen→winnt32/checkupgradeonly
- 2) Download des Programmes: Chkupgrd.exe von Microsoft (Readiness Analyzer RTW)

Clientcomputer unter Windows 95/98, die über inkompatible Hardware verfügen und daher W2K nicht ausführen können, können das Active Directory dennoch mit Hilfe des W2K-Verzeichnisdienst-Clients nutzen.

(Es wird dadurch der DFS-Dienst [Daten organisieren, die auf physisch mehreren Computern verteilt sind], ändern von Kennwörtern auf allen Domänencontrollern und das Durchsuchen von Active Directory unterstützt)

Vorraussetzung dafür ist der Internet-Explorer ab Version 4.0.1!

Um den Client auf einem Windows 95/98 zu installieren, muß man das Programm **Dsclient.exe** (**Windows2000 CD** im **Ordner \Client\Win9x**) ausführen.

(Syntax:  $Start \rightarrow Ausführen \rightarrow \client\win9x\dsclient.exe \rightarrow OK$ )

## Aktualisieren auf Windows2000 Advanced Server:

Identifizieren der Serveraktualisierungspfade:

#### Domänencontroller:

WindowsNT 3.51/4.0 (PDC oder BDC) → Windows2000 (Domänencontroller)

#### <u>Mitgliedsserver</u>

WindowsNT 3.51/4.0 (Mitgliedsserver) → Windows2000 (Mitgliedsserver)

→ Windows2000 (Domänencontroller) (optional)

#### Windows

WindowsNT 3.1/3.5  $\rightarrow$  WindowsNT 3.51/4.0  $\rightarrow$  Windows2000

#### Sichern wichtiger Datendateien und Einstellungen vor der Aktualisierung:

- Beheben von in der Ereignisanzeige aufgelisteten Fehlern
- Sichern aller Laufwerke
- Sichern der Registrierung (Um die Registry ohne Band zu sichern, muß Regback.exe im WindowsNT Resource Kit ausgeführt werden. Diese Datei sichert alles, bis auf den aktuell angemeldeten User. Um die Registry wieder herzustellen muß Regrest.exe, welche sich ebenfalls im WindowsNT Resource Kit befindet, ausgeführt werden.)
- Aktualisieren der Notfalldiskette (ERD Emergency Repair Disk) durch Ausführen von Rdisk.exe an der Eingabeaufforderung.
- Entfernen aller Virenscanner, der Netzwerkdienste von Drittanbietern, sowie der gesamten Clientsoftware
- Trennen serieller Kabel zur USV und aller Komponenten an COM1 und COM2 (außer Maus)
- Reservieren der Unterbrechungsanforderungen für nicht Plug&Play-fähige ISA-Geräte

#### Installieren von Hardware unter Windows2000:

In den meisten Fällen erkennt W2K das neue Hardwaregerät nach dem Anschließen per PnP automatisch. Falls dies nicht der Fall sein sollte, kann die neue Hardware unter der Option **Hardware** in der **Systemsteuerung** hinzugefügt werden.

Ist das hinzuzufügende Gerät in der HCL aufgenommen und somit von Microsoft zertifiziert, installiert W2K den Treiber automatisch.

Zum Installieren eines Gerätes muß man als Administrator oder als Mitglied der Gruppe Administratoren angemeldet sein.

Im Rahmen des Konfigurationsprozesses weist W2K dem zu installierenden Gerät einen eindeutigen Satz von Systemressourcen zu:

- Leitungsnummern für Interruptanforderungen (Interrupt Request, IRQ)
- DMA-Kanäle (Direct Memory Access)
- E/A-Anschlussadressen (Eingabe/Ausgabe Ports)
- Adressbereiche für den Arbeitsspeicher

Für ein nicht Plug&Play-fähiges Gerät, müssen die Ressourceneinstellungen bei Bedarf manuell im Gerätemanager konfiguriert werden.

Im Allgemeinen sollte man Ressourceneinstellungen nicht manuell ändern, da diese sonst zu festen Einstellungen werden und die Flexibilität von W2K dadurch eingeschränkt wird.

#### Aktualisieren von Treibern:

Es können nur Benutzer mit den entsprechenden Rechten (Administratoren) Treiber ändern.

System  $\to$  Hardware  $\to$  Geräte-Manager  $\to$  rechte Maustaste auf das zu aktualisierende Gerät  $\to$  Eigenschaften  $\to$  Treiber  $\to$  Treiber aktualisieren

## Verwalten der Treibersignierung:

Um die Stabilität des Betriebssystemes zu gewährleisten, werden Hardware-Treiber von Microsoft getestet und bei Bestehen zertifiziert (Windows Hardware Quality Labs – WHQL). Diese Treibersignierungen werden in einer Katalogdatei (CAT) gespeichert, auf welche in der zugehörigen INF-Datei des Hardware-Treibers verwiesen wird.

## Konfiguration der Treibersignierungsoptionen:

Arbeitsplatz  $\rightarrow$  Eigenschaften  $\rightarrow$  Hardware  $\rightarrow$  Treibersignierung

#### Ermitteln unsignierter Dateien:

Start  $\rightarrow$  Ausführen  $\rightarrow$  **sigverif** 

#### Hardwareprofile:

Ein Hardwareprofil legt die Konfiguration und die Charakteristika bestimmter Hardwaregeräte und –dienste und Einstellungen fest, welche beim Start geladen werden.

#### Erstellen des Hardwareprofils:

 $Start \rightarrow Einstellungen \rightarrow Systemsteuerung \rightarrow System \rightarrow Hardware \rightarrow Hardwareprofile$ 

- bestehendes Hardwareprofil kopieren
- Computer mit dem neuen Profil starten
- Im Gerätemanager die Dienste und Treiber konfigurieren

#### Konfigurieren der Anzeigeoptionen:

Um die Bildschirmfrequenz und -auflösung zu ändern ist folgende Lösung von Microsoft zu berücksichtigen:

 $Start \rightarrow Einstellungen \rightarrow Systemsteuerung \rightarrow Anzeige \rightarrow Einstellungen \rightarrow Erweitert$ 

Unter Monitor/Monitoreinstellungen werden die zu ändernden Frequenzen und Auflösungen ausgewählt. (**nicht** unter Grafikkarte/Alle Modi auflisten)

#### Konfigurieren mehrerer Monitore:

Es können bis zu 10 Monitore konfiguriert werden, allerdings sind dazu entweder **PCI-oder AGP-Grafikkarten** notwendig!

 $Start \rightarrow Einstellungen \rightarrow Systemsteuerung \rightarrow Anzeige \rightarrow Einstellungen \rightarrow auf das weitere Monitorsymbol, welches zusätzlich zum primären Monitor abgebildet wird, klicken <math>\rightarrow$  Windows-Desktop auf diesem Monitor erweitern aktivieren  $\rightarrow$  Übernehmen

Beim Starten des Computers dient der primäre Monitor als Mittelpunkt für alle Aktionen, auf welchem standardmäßig auch alle Anmeldedialoge angezeigt werden. Auch bei einem Programmstart wird dieses zuerst auf dem primären Monitor angezeigt und kann dann mit Hilfe der Maus auf die anderen Monitore verschoben werden.

## Konfigurieren von Systemeinstellungen:

 $Start \rightarrow Einstellungen \rightarrow Systemsteuerung \rightarrow System \rightarrow Systemeigenschaften \rightarrow Erweitert \rightarrow Umgebungsvariablen$ 

Konfigurierte Betriebssystemeinstellungen im Fenster "Umgebungsvariablen" gelten für das gesamte System und alle Benutzer eines Computers, dürfen aber nur von Administratoren erstellt, bzw. geändert werden. (Systemvariablen)

Benutzervariablen, welche sich ebenfalls im Fenster "Umgebungsvariablen" befinden, dürfen von jedem Benutzer erstellt, bzw. geändert werden und gelten nur für das jeweilige Benutzerprofil. (wird in seinem Benutzerprofil gespeichert) (Benutzervariablen)

Zu den Umgebungsvariablen des Benutzers gehören alle benutzerdefinierten Einstellungen (z.B.: Ordner Temp) und alle von Anwendungen definierten Variablen (z.B.: Pfad der Anwendungsdateien)

#### Umgebungsvariablen werden in folgender Reihe festgelegt:

- 1.) Variablen von Autoexec.bat
- 2.) Umgebungsvariablen des Systems
- 3.) Umgebungsvariablen des Benutzers

Die Einstellung der Umgebungsvariable eines Benutzers setzt die Einstellungen von System außer Kraft, welche wiederum die Einstellungen von Autoexec.bat außer Kraft setzt. (Voraussetzung: Es handelt sich um die gleiche definierte Variable.)

#### Ändern von Start- und Wiederherstellungsoptionen:

Start → Einstellungen → Systemsteuerung → System → Systemeigenschaften → Erweitert → Starten und Wiederherstellen

Mit diesen Optionen kann angegeben werden, welches Betriebssystem der Computer bei Start verwenden und welche Aktion(en) bei einer unerwarteten Beendigung des Systems ausgeführt werden soll.

#### Folgende Optionen sind für Wiederherstellungseinstellungen verfügbar:

- Eintrag im Systemprotokoll
- Administratorwarnmeldung senden
- Debuginformationen speichern
- Automatisch neu starten

#### Für die Debuginformationen gelten folgende Anforderungen:

- Die Auslagerungsdatei muß sich auf derselben Partition befinden, wie der Systemordner (am besten auf eine FAT-Partition auslagern)
- Die Auslagerungsdatei muß um 1MB größer sein, als der physische Arbeitsspeicher (RAM) des Computers
- Auf dem Datenträger muß genug freier Speicherplatz für die angegebene Datei verfügbar sein. (Achtung: um eine vorherige Systemfehlerdatei zu überschreiben, muß das Kontrollkästchen "Bereits vorhandene Datei überschreiben" aktiviert sein.)

#### Konfigurieren der Desktopumgebung:

Die Systemsteuerung kann zum Ändern der Darstellung und der Funktionsweise von W2K verwendet werden. Mit ihrer Hilfe ist es möglich, Benutzeranforderungen (Ländereinstellungen, Währungen, Datum, Zahlen, Uhrzeit, Eingabe, Körperbehinderungen des Benutzers, Installation + Entfernen + Ändern + Reparieren von Anwendungen...) einzustellen.

#### Konfigurieren von Eingabegebietsschemas (Ländereinstellung):

- 1) Standardeinstellung
- 2) Gebietsschema
- 3) Zusätzliche Sprache

#### Konfigurieren von Eingabehilfen:

Es gibt zwei Arten von Hilfsprogrammen: 1) Eingabehilfsprogramme und 2) Eingabehilfen

- 1) Start → Programme → Zubehör → Eingabehilfen
  - Bildschirmlupe
  - Microsoft Sprecher
  - Bildschirmtastatur
  - Hilfsprogramm-Manager (nur vom Administrator einzustellen)
- 2) Start  $\rightarrow$  Einstellungen  $\rightarrow$  Systemsteuerung  $\rightarrow$  Eingabehilfen
  - hier werden Tastatur-, Bildschirm- und Mausfunktionen festgelegt

Um Optionen und Programme gemäß individuellen Bedürfnissen einzurichten und die Konfiguration in einer Datei speichern und diese auf andere Computer übertragen zu können, wird der Eingabehilfen-Assistent benötigt.

 $Start \rightarrow Programme \rightarrow Zubehör \rightarrow Eingabehilfen \rightarrow Eingabehilfen-Assistent$ 

## Verwalten von Anwendungen:

- 1) **Vorbereitung:** Identifizieren von Produkten, die unter W2K eingesetzt werden können
- 2) Installation: Installieren von Anwendungen mit Hilfe von "Software"

 $(Start \rightarrow Einstellungen \rightarrow Systemsteuerung \rightarrow Software)$ 

Anwendungen, die in **Software** im Abschnitt **Programme aus dem Netzwerk hinzufügen** angezeigt werden, verfügen über eine zugehörige MSI-Datei und wurden im Active Directory-Verzeichnisdienst veröffentlicht, damit Domänenmitglieder diese nach der Veröffentlichung installieren können.

Mit Hilfe von **Software**, Windows Explorer oder der Eingabeaufforderung können Windows Installer-Pakete (MSI-Dateien), welche man mit WinInstall LE erstellt, bereitgestellt werden.

3) **Verwaltung:** Verwalten von Anwendungen mit Hilfe von "Software" (Start → Einstellungen → Systemsteuerung → Software)

#### Konfigurieren von Internetoptionen für Clientcomputer:

 $(Start \rightarrow Einstellungen \rightarrow Systemsteuerung \rightarrow Internetoptionen$ oder im Internet Explorer  $\rightarrow$  Extras  $\rightarrow$  Internetoptionen)

Zu den typischen konfigurierenden Einstellungen gehören:

- Startseite des Browsers
- Gesamter für temporäre Internetdateien verwendete Speicherplatz
- Proxyserver zwischen dem LAN und dem Internet
- Sicherheitsebenen (4 verschiedene Sicherheitsebenen möglich)

Um den Internet Explorer für die Verwendung eines Proxyservers zu konfigurieren, ist folgender Schritt notwendig:

 $Start \rightarrow Einstellungen \rightarrow Systemsteuerung \rightarrow Internetoptionen \rightarrow Verbindungen \rightarrow LAN-Einstellungen \rightarrow Proxyserver verwenden \rightarrow Adresse und Anschluß eingeben$ 

Um die Leistung für Intranetwebsites zu erhöhen, muß das Kontrollkästchen **Proxyserver** für lokale Adressen umgehen aktiviert werden!

#### Netzwerke unter Windows 2000:

Ein Netzwerk setzt sich aus mehreren, untereinander kommunizierenden Computern zusammen. Um sich untereinander zu sehen und zu verstehen, werden sogenannte Protokolle (TCP/IP und IPX) eingesetzt.

Es werden 4 Komponenten verwendet, um eine Verbindung zu einem Netzwerk herzustellen:

- 1) Netzwerkadapter
- 2) Protokolle (Netzwerk-)
- 3) Netzwerkdienste
- 4) Bindungen (2mal; zwischen 1 + 2 und 2 + 3)

(siehe Bild Unterrichtseinheit 3 / Seite 2)

Netzwerkadapter: eine Hardwarekomponente, die eine Schnittstelle zwischen Computer

und Netzwerkkabel darstellt.

Protokolle: eine Reihe von Regeln und Konventionen (Inhalt, Format, zeitlicher

Ablauf, Reihenfolge, Fehlerkontrolle) zum Senden und Empfangen

von Daten.

Netzwerkdienste: ermöglichen Computern, auf denen dieselben Netzwerkprotokolle

ausgeführt werden, das Herstellen einer Verbindung. Unter W2K wird der Client für MS-Netzwerke automatisch installiert, Gateway und Client Services für NetWare muß dagegen manuell nachinstalliert

werden.

**Bindungen:** Methode zum Verknüpfen von Netzwerkkomponenten

(Netzwerkadapter und Protokoll, bzw. Protokoll und Netzwerkdienste).

#### Herstellen einer Verbindung zu einem Microsoft-Netzwerk:

Wenn ein Netzwerkadapter erkannt wurde, installiert W2K automatisch den Client für MS-Netzwerke, die Datei- und Druckerfreigabe für MS-Netzwerke und das TCP/IP-Protokoll (für DNS, DHCP und Active Directory) bei der Installation.

(rechte Maustaste auf Netzwerkumgebung  $\rightarrow$  Eigenschaften  $\rightarrow$  im Fenster Netzwerk- und DFÜ-Verbindung mit rechter Maustaste auf Symbol der zur konfigurierenden LAN-Verbindung klicken  $\rightarrow$  Eigenschaften)

Ein Clientcomputer besitzt zwei Möglichkeiten, seine IP-Adresse automatisch zu beziehen:

#### 1) von einem DHCP-Server

Ein DHCP-Server stellt automatisch eine IP-Adresse und weitere TCP/IP-Konfigurationsinformationen (z.B.: IP-Adresse des DNS- und WINS-Servers und das Standardgateway) bereit.

(der Clientcomputer fordert vom DHCP-Server eine IP-Adresse an, die dieser dem Client anschließend zur Verfügung stellt)

#### 2) über die automatische private IP-Adressierung (APIPA)

Falls kein DHCP-Server zur Verfügung steht, stellt die APIPA nur eine IP-Adresse und eine Subnetzmaske, jedoch keine zusätzlichen Konfigurationsinformationen (wie bei einem DHCP-Server) bereit. Dadurch wird die Verbindung des Clients zum LAN eingeschränkt. (Keine Verbindung zu anderen Netzwerken und Internet)

Wird ein Computer ohne IP-Adresse gestartet, geschieht folgendes:

- 1) Der Clientcomputer versucht einen DHCP-Server zu finden um seine Informationen zu erhalten
- 2) Wird kein DHCP-Server gefunden, konfiguriert der Client automatisch die zugehörige IP-Adresse und Subnetzmaske unter Verwendung einer ausgewählten Adresse des von Microsoft reservierten B-Klasse-Netzwerkes. (IP 169.254.0.0 / Subnet: 255.255.0.0)

#### Vergeben einer statischen IP-Adresse:

(rechte Maustaste auf Netzwerkumgebung  $\rightarrow$  Eigenschaften  $\rightarrow$  im Fenster Netzwerk- und DFÜ-Verbindung mit rechter Maustaste auf Symbol der zur konfigurierenden LAN-Verbindung klicken  $\rightarrow$  Eigenschaften)

Um eine statische Netzwerk-Adresse zu definieren, müssen folgende Parameter beachtet werden:

- IP-Adresse: diese identifiziert den Clientcomputer im Netzwerk

- Subnetzmaske: gibt an, welcher Teil einer IP-Adresse die Netzwerkkennung

und welcher die Hostkennung darstellt.

- Standardgateway: vermittelt Daten unter den verschiedenen Subnetzen, da er

alle an ihm angeschlossenen Netzwerksegmente kennt.

**Achtung:** Wenn mindestens zwei Computer über dieselbe IP-Adresse verfügen, zeigt W2K auf beiden Rechnern eine Warnmeldung an und deaktiviert TCP/IP auf diesen!

## Überprüfen und Testen einer TCP/IP-Konfiguration:

Um sicherzustellen, daß der Computer mit Hilfe von TCP/IP mit einem Netzwerk kommunizieren kann, müssen folgende Punkte beachtet werden:

 Ipconfig: es wird geprüft, ob der Computer für TCP/IP initialisiert ist. Daraufhin werden die IP-Adresse, die Subnetzmaske und das Standardgateway des Rechners angezeigt.

Sofern eine doppelte IP-Adresse vorhanden ist, wird zwar diese richtig, allerdings die Subnetzmaske nur mit 0.0.0.0 angezeigt.

Eine automatische private IP-Adresse hat grundsätzlich die Netzwerkkennung 169.254.0.0.

- Ping: mit **ping 127.0.0.1** wird die **Loopbackadresse** ausgegeben, welche der Computer verwendet, um zu überprüfen, ob TCP/IP ordnungsgemäß installiert ist und um sich selbst zu identifizieren.

Anschließend sollten einige bekannte IP-Adressen (Server, Gateway, andere, bzw. eigenen Rechner im Netzwerk, Remotehost) angepingt werden, um die einwandfreie Netzwerkkommunikation zu testen.

#### Herstellen einer Verbindung zu einer Netzwerkressource unter W2K:

Zum Herstellen einer solchen Verbindung bietet Windows 2000 mehrere Möglichkeiten:

- 1) Internet Explorer
- 2) Ausführen (Pfad zu den Netzwerkressourcen muß eingegeben werden)
- 3) Netzlaufwerk verbinden
- 4) Netzwerkumgebung
- 5) Suchen (Computer suchen)

#### Herstellen einer Verbindung zu einem Novell NetWare-Netzwerk:

Um einen W2K-Client mit einem NetWare-Netzwerk (IPX/SPX) zu verbinden, muß das NWLink-Protokoll, der Client-Service und Gateway Services (bei W2k Advanced Server) für NetWare installiert werden.

- Das NWLink-Protokoll ermöglicht W2K-Computern den Zugriff auf Anwendungen, die auf einem Novell Net-Ware-Server ausgeführt werden. (Client Service für NetWare für Clientcomputer ist hier nicht erforderlich)
- Client Service für NetWare ist ein Dienst, der Clientcomputern, auf denen W2K-Professional und NWLink ausgeführt werden, das Herstellen einer Verbindung zu Netzwerkressourcen, wie Datei- und Druckerressourcen, auf einem Novell NetWare-Server ermöglicht.
- Gateway Service ermöglicht W2K-Computern das Herstellen einer Verbindung zu einem freigegebenen Ordner auf einem Novell NetWare-Server, indem über den W2K-Server, auf dem Gateway Service für NetWare ausgeführt wird, eine Verbindung hergestellt wird. (Client Service für NetWare für Clientcomputer ist hier nicht erforderlich)

(siehe Bild: Unterrichtseinheit 3 / Seite 25)

## Installation und Konfiguration von NWLink:

(rechte Maustaste auf Netzwerkumgebung  $\rightarrow$  Eigenschaften  $\rightarrow$  im Fenster Netzwerk- und DFÜ-Verbindung mit rechter Maustaste auf Symbol der zur konfigurierenden LAN-Verbindung klicken  $\rightarrow$  Eigenschaften)

Bei der Installation des NWLink erkennt W2K automatisch den Rahmentyp und die Netzwerknummer.

Eine interne Netzwerknummer, welche einen Server in einem IPX-Netzwerk eindeutig identifiziert (vergleichbar mit dem Hostanteil einer IP-Adresse), muß in folgenden Fällen noch manuell zugewiesen werden:

- File und Print Services für NetWare sind installiert und es sind mehrere Rahmentypen auf einem einzigen Adapter vorhanden, bzw. NWLink ist mit mehreren Adaptern des Computers verbunden.
- Eine Anwendung verwendet das NetWare-Protokoll SAP. (z.B.: wenn SQL- und SNA-Server als Anwendungen auf Novell laufen)

#### Konfiguration eines Rahmentyps:

Bei der Installation von NWLink (wird automatisch bei der Installation von Gateway Services mitinstalliert) bestimmt W2K automatisch, welcher Rahmentyp im Netzwerk verwendet wird und legt diesen entsprechend fest. Werden mehrere Rahmentypen erkannt, wird standardmäßig der Rahmentyp 802.2 von NWLink verwendet. In einem solchen Fall müssen alle erforderlichen Rahmentypen und Netzwerknummern manuell (mit dem Befehl: ipxroute config) konfiguriert werden.

#### Konfiguration einer Netzwerknummer:

Die Netzwerknummer ist mit der Subnetzmaske in der TCP/IP-Konfiguration vergleichbar. Alle Computer in einem Segment, die denselben Rahmentyp verwenden, müssen auch dieselbe Netzwerknummer verwenden, um miteinander zu kommunizieren.

#### Herstellen einer Verbindung zu einer NetWare-Netzwerkressource:

Zum Herstellen einer solchen Verbindung bietet Windows 2000 mehrere Möglichkeiten:

- 1) Internet Explorer
- 2) Netzlaufwerk verbinden
- 3) Netzwerkumgebung

#### Erstellen und Verwalten von Benutzerkonten:

Benutzerkonten enthalten eindeutige Informationen eines Benutzers und ermöglichen diesem die Anmeldung und somit den Zugriff auf lokale und Domänen-Ressourcen. (Ist man mit einem normalen Benutzeraccount angemeldet, kann man trotzdem als Administrator fungieren:  $Start \rightarrow Einstellungen \rightarrow Systemsteuerung \rightarrow System \rightarrow Verwaltung \rightarrow mit rechter Maustaste und gedrückter Umschalttaste auf Active Directory-Benutzer und -Computer klicken <math>\rightarrow$  Ausführen als)

#### Lokale Benutzerkonten:

ermöglichen einem Benutzer die Anmeldung an einem bestimmten Computer, um Zugriff auf dessen Ressourcen zu erhalten. Die Benutzerkonten befinden sich im SAM des Computers.

#### Domänenbenutzerkonten:

ermöglichen einem Benutzer die Anmeldung an einer Domäne, um Zugriff auf Netzwerkressourcen zu erhalten. Die Domänenbenutzerkonten befinden sich im Active Directory.

#### Vordefinierte Benutzerkonten:

ermöglichen einem Benutzer die Ausführung von Verwaltungsaufgaben, bzw. den temporären Zugriff auf Netzwerkressourcen. Diese Konten befinden sich sowohl im SAM (vordefinierte lokale Benutzerkonten), als auch im Active Directory (vordefinierte Domänenbenutzerkonten).

Es stehen zwei vordefinierte Benutzerkonten zur Verfügung, die nicht gelöscht werden können: **Administrator** und **Gast**. Diese werden automatisch während der Installation von W2K und Active Directory erstellt.

#### Namenskonventionen:

Die Namenskonvention legt fest, wie Benutzerkonten in der Domäne identifiziert werden.

- Benutzeranmeldenamen müssen im Active Directory, vollständige Namen innerhalb der Domäne und lokale auf dem Computer eindeutig sein.
- Benutzeranmeldenamen können eine Kombination aus bis zu 20 speziellen und alphanumerischen Zeichen, sowohl in Groß-, als auch in Kleinschreibung enthalten. (Ausnahmen: ""/\[]:; |=, + \*? < >)
- die Namenskonvention sollte Benutzer, welche den gleichen Namen besitzen und temporäre Benutzer identifizieren können

#### Kennwortrichtlinien:

Um den Zugriff auf die Domäne oder einen Computer zu schützen, sollte jedem Benutzerkonto ein komplexes Kennwort zugewiesen werden.

- dem Konto Administrator sollte stets ein Passwort zugewiesen werden, um unautorisierten Zugriff zu verhindern
- der Administrator legt fest, ob Benutzer das Kennwort selbständig ändern können oder nicht
- es können bis zu 128 Zeichen mit einer Kombination aus Groß- und Kleinbuchstaben, sowie aus speziellen und alphanumerischen Zeichen verwendet werden. (Mindestlänge von 8 Zeichen in komplexer Form wird empfohlen)

#### Kontooptionen:

Benutzerkontooptionen legen fest, wie ein Benutzer auf die Domäne oder einen Computer zugreifen kann.

- die Anmeldezeiten sollten nach den Arbeitszeiten des Benutzers festgelegt werden
- um die Sicherheit zu erhöhen, können Domänenbenutzer auf bestimmte Computer eingeschränkt werden; standardmäßig können sie sich an jedem Computer der Domäne anmelden
- es kann eine Ablaufzeit für ein Benutzerkonto festgelegt werden, damit sich dieses automatisch nach dem Ablaufdatum deaktiviert

#### Erstellen eines lokalen Benutzerkontos:

Ein lokales Benutzerkonto wird nur in kleineren Netzwerkumgebungen, wie Arbeitsgruppen, oder alleinstehenden Computern, welche nicht an ein Netzwerk angeschlossen sind, verwendet. Es wird in der SAM-Datenbank des Computers gespeichert und ermöglicht dem Benutzer, auf seine lokalen Ressourcen zugreifen zu können.

(Start o Programme o Verwaltung o Computerverwaltung o erweitern von Lokale Benutzern und Gruppen o rechte Maustaste auf Benutzer o Neuer Benutzer o Kennwort eingeben und bestätigen o Kennworteinschränkungen festlegen o Erstellen)

## Verwaltungsprogramme von Windows 2000:

Verwaltungsprogramme (befinden sich auf der W2K-Server CD und sind standardgemäß auf einem Domänencontroller installiert) für die Remoteverwaltung von Domänencontrollern (nur mit Administratorrechten möglich) können von jedem W2K-Rechner aus installiert werden.

(Explorer → Ordner I386 → Adminpak.msi → nach der Installation : Start → Programme → Verwaltung)

(Aus Sicherheitsgründen sollte man sich als normaler Benutzer anmelden und sich für die Verwaltungsaufgaben mit **Ausführen als** als Administrator verbinden lassen)

#### Erstellen eines Domänenbenutzerkontos:

Ein Domänenbenutzerkonto befindet sich auf einem Domänencontroller und wird automatisch auf alle anderen Domänencontroller repliziert).

Um ein Domänenbenutzerkonto (im Standardordner Users) zu erstellen, muß folgendes beachtet werden:

- öffnen des Active Directory-Benutzer und -Computer vom Menü Verwaltung aus
- rechte Maustaste auf den Ordner, der das Benutzerkonto enthalten soll, dann auf Neu und User klicken.

#### Konfigurierbare Optionen:

Vorname / Nachname / Initialen

Vollständiger Name: dieser Name muß innerhalb des Ordners, in dem das (des Benutzers)

Konto erstellt wird, eindeutig sein.

(W2K vervollständigt diesen Eintrag selbständig, wenn

der Vor- und Nachname eingegeben wurde)

Benutzeranmeldename: dieser eindeutige Anmeldename des Benutzers ist er-

forderlich und muss im Active Directory eindeutig sein. Benutzeranmeldenamen für WindowsNT 3.5x/4.0 werden verwendet, um eine Anmeldung von vorherigen Versionen von Windows durchzuführen und müssen innerhalb der Domäne eindeutig sein (max. 20 Zeichen)

#### Verwalten von Benutzerdaten durch das Erstellen von Basisordnern:

Bei den Basisordnern für Benutzer handelt es sich um einen zentralen Netzwerkspeicherort für jeden einzelnen User.

Beim Festlegen dieses Basisordners sollten folgende Punkte berücksichtigt werden:

- um Datenverluste zu verhindern, ist eine Datensicherung/-wiederherstellung unvermeidlich. Um viel effizienter arbeiten zu können, empfiehlt es sich, die Dateien an einem zentralen Speicherort auf einem Server abzulegen.
- auf dem Server muß genügend Speicherplatz für die Benutzerdaten zur Verfügung stehen. Durch die Datenträgerkontingente bietet W2K eine präzise Kontrolle über den zu verwendenden Festplattenspeicherplatz.
- es muß auf dem Benutzercomputer ausreichend Speicherplatz vorhanden sein.
- befindet sich der Basisordner auf dem lokalen Computer des Benutzers, so entsteht zwar weniger Netzwerkverkehr, macht aber eine zentrale Datensicherung durch den Administrator nahezu unmöglich.

#### Eigenschaften für Domänenbenutzerkonten:

Um im Active Directory nach Benutzern zu suchen, können definierte Eigenschaften im Domänenbenutzerkonto angegeben werden. Man kann z.B. nach einer Person suchen, indem man als Kriterium die Telefonnummer, den Arbeitsplatz, den Namen des Vorgesetzten oder den Nachnamen eingibt. Aus diesem Grund sollten für jedes Domänenbenutzerkonto, welches erstellt wird, detaillierte Eigenschaftsdefinitionen angegeben werden.

Um diese persönlichen Eigenschaften festzulegen, müssen folgende Schritte ausgeführt werden:

- öffnen des Active Directory-Benutzer und -Computer vom Menü Verwaltung aus
- Domäne auswählen und auf entsprechenden Ordner klicken, um die verfügbaren Domänenbenutzerkonten anzuzeigen
- rechte Maustaste auf das jeweilige Domänenbenutzerkonto
- **Eigenschaften** und dann die jeweilige Registerkarte auswählen

#### Eigenschaften für Domänenbenutzerkonten:

Das Festlegen von Anmeldeoptionen für ein Domänenbenutzerkonto ermöglicht, die Anmeldezeiten (sinnvoll vor allem in einem Regierungsnetzwerk und in Umgebungen mit mehreren Schichten) und die Computer, in, bzw. von denen sich ein Benutzer anmelden kann, zu steuern.

Verbindungen zu Netzwerkressourcen in der Domäne werden allerdings nicht getrennt, wenn die Anmeldezeiten des Benutzers ablaufen. Der Benutzer kann jedoch keine neuen Verbindungen zu anderen Computern in der Domäne herstellen.

## Kopieren von Domänenbenutzerkonten:

Es kann nur ein Benutzerkonto auf einem Domänencontroller, nicht aber auf einem W2K-Computer kopiert werden.

Folgende Eigenschaften werden beim Kopieren in das neue Benutzerkonto übertragen:

- Allgemein / Rufnummern: es werden keine Eigenschaften kopiert

- Adresse: alle außer Straße

Konto: alle außer Anmeldename

- **Profil**: alle außer Profilpfad und Basisordner

- **Organisation**: alle außer Anrede

- Mitglied von: alle

- Einwählen / Umgebung / Sitzungen / Remoteüberwachung / Terminaldienstprofile: es werden keine Eigenschaften kopiert, sondern nur Standardeinstellungen angewendet.

Achtung: Rechte und Berechtigungen, die einem einzelnen Benutzerkonto erteilt werden, werden nicht in das neue Benutzerkonto kopiert!

#### Erstellen von Benutzerkonten (User Template):

Eine Benutzerkontenvorlage (Domänenbenutzerkonto, in dem das Kontrollkästchen **Konto ist deaktiviert** aktiviert ist) ist ein Standardbenutzerkonto, welches die Eigenschaften enthält, die auf Benutzer mit gemeinsamen Anforderungen angewendet werden.

Bei der Erstellung von Vorlagen sind folgende Richtlinien zu beachten:

- es sollte eine Vorlage für jede Klassifizierung von Mitarbeitern erstellt werden
- für Mitarbeiter, die das Netzwerk nur für kurze Zeit oder temporär nutzen, sollte eine Vorlage mit beschränkten Anmeldezeiten, Arbeitsstationsspezifikationen und anderen notwendigen Beschränkungen erstellt werden

Um die Vorlage stets oben in der Liste im Detailfensterbereich des **Active Directory-Benutzer und –Computer** anzeigen zu lassen, sollte man die Vorlagenamen mit einem \_ beginnen lassen.

Um eine Vorlage zur Erstellung eines neuen Benutzerkontos zu verwenden, wird das Vorlagenkonto kopiert und ein Benutzername, ein Kennwort und die entsprechenden Änderungen in den Benutzerkontoeigenschaften eingestellt. Das Kontrollkästchen **Konto ist deaktiviert** muss deaktiviert werden, um das Benutzerkonto dem Benutzer zur Verfügung zu stellen.

#### <u>Anpassen von Benutzereinstellungen mit Benutzerprofilen</u>

Unter W2K wird die Computerumgebung eines Benutzers hauptsächlich durch das Benutzerprofil bestimmt, da dieses alle Einstellungen, welche der Benutzer für seine Arbeitsumgebung benötigt, enthält.

Ein solches Benutzerprofil wird erstellt, wenn sich ein Benutzer zum ersten Mal an einem Computer anmeldet. Alle benutzerspezifischen Einstellungen werden automatisch im Ordner des Benutzers innerhalb des Ordners C:\Dokumente und Einstellungen\Benutzername gespeichert.

Die Aktualisierung des Profils auf dem Computer erfolgt beim Abmelden des Benutzers.

#### **Profiltypen:**

Standardbenutzerprofil: dient als Basis für alle Benutzerprofile. Den Anfang für jedes

Benutzerprofil bildet eine Kopie des Standardbenutzerprofils,

das auf jedem Computer unter W2K gespeichert ist.

Lokales Benutzerprofil: wird erstellt und auf dem lokalen Computer gespeichert, wenn

sich ein Benutzer zum ersten Mal an einem Computer anmeldet. Alle Änderungen, die am lokalen Benutzerprofil vorgenommen werden sind spezifisch für den Computer, an dem die Änderungen vorgenommen wurden. Auf einem Computer können mehrere lokale Benutzerprofile vorhanden

sein.

Servergespeichertes Benutzerprofil: wird vom Systemadministrator erstellt und auf

einem Server gespeichert. Dieses Profil ist jedes Mal verfügbar, wenn sich ein Benutzer an einem Computer im Netzwerk anmeldet. Bei Änderungen des Profils werden diese beim Abmelden im

Benutzerprofil auf dem Server aktualisiert.

**Verbindliches Benutzerprofil:** wird vom Systemadministrator erstellt, um eine

bestimmte Einstellung für Benutzer anzugeben. Dieses Profil kann sowohl lokal-, als auch servergespeichert sein. Ein verbindliches Benutzerprofil ermöglicht einem Benutzer zwar, Änderungen an seinen Desktopeinstellungen

vorzunehmen, diese aber nicht zu speichern.

#### Erstellen eines servergespeicherten Benutzerprofils:

1) Erstellen eines freigegebenen Ordners (mit der Berechtigung Vollzugriff) auf einem Server

2) Angabe des Pfades für diesen Ordner.

Start o Einstellungen o Systemsteuerung o System o Verwaltung o Active Directory-Benutzer und -Computer o mit rechter Maustaste auf entsprechendes Benutzerkonto klicken o Eigenschaften o Profil o im Benutzerprofil die Pfadinformationen

(\lServername\Name \des \freigegebenen \operactor \rangle \text{Benutzername}) \rightarrow \text{Profilpfad} \text{Statt Benutzername kann die Variable \mathbb{\circ}\username\circ\unders\text{Benutzername} \text{angegeben werden, da W2K diese automatisch mit dem Benutzerkontennamen f\u00fcr das servergespeicherte Profil ersetzt.

Ein servergespeichertes Benutzerprofil kann nur von einem Administrator geändert werden. Die Datei **Ntuser.dat** (im Profilordner des Benutzers) enthält den Abschnitt der Registrierung, der für das Benutzerkonto (Benutzerprofileinstellungen) gilt.

## Erstellen eines verbindlichen servergespeicherten Benutzerprofils:

- 1) Erstellen eines freigegebenen Ordners mit einem Profilordner (mit der Berechtigung Vollzugriff) für das Benutzerprofil auf einem Server.
- 2) Ein konfiguriertes, servergespeichertes Benutzerprofil einrichten, indem ein neuer Benutzer im **Active Directory-Benutzer und –Computer** erstellt und darin die Pfadangabe aus 1) eingestellt wird.
  - Um dieses Profil zu konfigurieren ist es notwendig, sich an der Domäne mit dem eben erstellten Profil anzumelden, die Einstellungen vorzunehmen und sich anschließend wieder abzumelden.
- 3) Die Profildatei **Ntuser.dat** muss nun in **Ntuser.man** umbenannt werden, da hiermit das Profil schreibgeschützt und somit verbindlich wird.

Die Datei Ntuser.dat wird im Profilordner des Benutzers nicht angezeigt.

Um sie anzuzeigen, müssen folgende Schritte ausgeführt werden:

Windows Explorer starten  $\rightarrow$  Extras  $\rightarrow$  Ordneroptionen  $\rightarrow$  Ansicht  $\rightarrow$  Erweiterte Einstellungen  $\rightarrow$  Alle Dateien und Ordner anzeigen  $\rightarrow$  das Kontrollkästchen "Dateinamenerweiterung bei bekannten Dateitypen ausblenden" deaktivieren  $\rightarrow$  OK

#### Optimale Methoden für das Erstellen und Verwalten von Benutzerprofilen:

- Umbenennen des Administratorkontos
- Erstellen eines Benutzerkontos mit Administratorrechten
- Erstellen eines Benutzerkontos für nicht administrative Aufgaben
- Aktivieren des Kontos "Gast" mit Vergabe eines Passwortes nur in Netzwerken mit niedriger Sicherheit
- Erstellen zufälliger anfänglicher Kennwörter
- Auffordern von neuen Benutzern, ihre Kennwörter zu ändern
- Festlegen von Benutzerkonto-Ablaufdaten für temporäre Mitarbeiter

#### Arbeitsweise von Windows 2000 Gruppen:

Eine Gruppe ist eine Sammlung von Benutzerkonten, um Zugriffsberechtigungen auf gleiche Ressourcen zu vereinfachen, wobei diese in einer Arbeitsgruppe anders als in einer Domäne arbeitet.

Beim Hinzufügen von Mitgliedern zu Gruppen sollte jedoch folgendes beachtet werden:

- wird ein Benutzer Mitglied einer Gruppe, so erhält er alle Rechte (Tätigkeiten, die ich ausführen kann) und Berechtigungen (Zugriffsrechte im NTFS-Dateisystem), die der Gruppe erteilt werden
- da eine Gruppe nur eine Liste der Mitglieder mit Verweisen auf die tatsächlichen Benutzerkonten ist, können Benutzerkonten Mitglieder mehrerer Gruppen sein

#### Gruppen in einer Arbeitsgruppe:

- sie werden auf Computern erstellt, die keine Domänencontroller sind
- sie befinden sich in der Sicherheitskontenverwaltung (SAM), welche die lokale Datenbank für Sicherheitskonten des Computers ist
- sie werden verwendet, um Berechtigungen für Ressourcen und Systemtasks auf dem Computer zu erteilen, auf dem die Gruppe erstellt ist

## Gruppen in einer Domäne:

- sie werden nur auf Domänencontrollern erstellt
- sie befinden sich im Active Directory Verzeichnisdienst
- sie werden verwendet, um Berechtigungen für Ressourcen und Systemtasks auf allen Computern der Domäne zu erteilen

#### Lokale Gruppen:

#### - Richtlinien für lokale Gruppen:

- lokale Gruppen werden nur auf Computern eingerichtet, die zu keiner Domäne gehören
- lokale Gruppen werden verwendet, um den Zugriff auf Ressourcen zu steuern und um Systemtasks für den lokalen Computer durchzuführen

#### - Regeln für die Mitgliedschaft in lokalen Gruppen:

- lokale Gruppen können nur lokale Benutzerkonten des lokalen Computers enthalten, auf dem sie erstellt wurden
- lokale Gruppen können nicht Mitglieder einer anderen Gruppe sein

Gruppen können nur von Mitgliedern der Gruppe Administratoren oder Konten-Operatoren erstellt werden.

#### Integrierte lokale Gruppen:

Integrierte Gruppen werden bei der Installation von W2K automatisch angelegt. Sie haben eine Reihe von vorbestimmten Rechten und können nicht gelöscht werden.

#### - Integrierte lokale Gruppen:

- über diese Gruppen erhalten deren Mitglieder die Rechte, Systemtasks auszuführen
- ein Hinzufügen von Benutzerkonten ist möglich

#### - Besondere Identitäten (Sondergruppen):

- über diese Gruppen werden die Systemverwendungen für Benutzer organisiert (z.B.: Administrator, Benutzer, Gast...)
- ihre automatische Mitgliedschaft kann nicht modifiziert werden (z.B.: Jeder, System...)

## <u>Strategie zum Verwenden von lokalen Gruppen in einer Arbeitsgruppe</u> (ALP-Strategie):

In einer Arbeitsgruppenumgebung ist die Strategie, welche zum Erteilen von Berechtigungen und Rechten verwendet wird, unkompliziert.

#### Die ALP-Strategie:

- Platzieren von Benutzerkonten (*Accounts A*) in einer lokalen Gruppe (*Lokal L*) auf dem lokalen Computer
- Erteilen von Berechtigungen (Permissions P) oder Rechten an die lokale Gruppe

## Erstellen von lokalen Gruppen:

Start  $\rightarrow$  Programme  $\rightarrow$  Verwaltung  $\rightarrow$  Computerverwaltung  $\rightarrow$  erweitern von Lokale Benutzern und Gruppen  $\rightarrow$  rechte Maustaste auf Gruppen  $\rightarrow$  Neue Gruppe

Achtung: Der Gruppenname (256 Zeichen bei W2k und 20 Zeichen bei WinNT) für die lokale Gruppe muss eindeutig sein.

## Implementieren von Gruppen in einer Domäne:

Mit Domänengruppen, welche auf einem Domänencontroller erstellt werden, ist eine zentrale Verwaltung in einer Domäne möglich. Windows 2000 erstellt auch hier bei der Installation automatisch integrierte Gruppen.

## Gruppentypen:

#### • Sicherheitsgruppen:

diese Gruppen werden für sicherheitsbezogene Aufgaben, wie das Erteilen von Berechtigungen für den Zugriff auf Ressourcen (oder Senden von E-Mail-Nachrichten an mehrere Benutzer), verwendet. **[für Personenberechtigungen]** 

#### • Verteilergruppen:

Anwendungen verwenden Verteilergruppen als Listen für nicht sicherheitsbezogene Funktionen (senden von E-Mail-Nachrichten an Benutzergruppen). Diese Gruppen können nicht zum Erteilen von Berechtigungen verwendet werden. **[für Software]** 

## Gruppenbereiche:

Der Bereich einer Gruppe (Gruppenbereich) bestimmt, wo diese in den Domänen verwendet wird und beeinflusst die Gruppenmitgliedschaft und das Verschachteln von Gruppen (eine Gruppe wird als Mitglied zu einer anderen Gruppe hinzugefügt).

#### <u>Unter Windows 2000 gibt es 3 Gruppenbereiche:</u>

### 1. Globaler Gruppenbereich

(zum Organisieren von Benutzern mit ähnlichen Anforderungen an den Netzwerkzugriff)

- Eingeschränkte Mitgliedschaft (nur Benutzerkonten und globale Gruppen, in der die globale Gruppe erstellt wird)
- Globale Gruppen können in anderen Gruppen verschachtelt sein

#### 2. Gruppenbereich der lokalen Domäne

(zum Erteilen von Berechtigungen für Domänenressourcen)

- Die Mitgliedschaft ist für alle Gruppen und Benutzerkonten offen
- Gruppen der lokalen Domäne können nicht in anderen Gruppen verschachtelt werden

#### 3. Universeller Gruppenbereich

(zum Erteilen von Berechtigungen für ähnliche Ressourcen in mehreren Domänen)

- Die Mitgliedschaft ist für alle Gruppen und Benutzerkonten offen
- Universelle Gruppen können in anderen Gruppen verschachtelt sein

Achtung: Sicherheitsgruppen mit einem universellen Gruppenbereich stehen nur zur Verfügung, wenn sich die Domäne im einheitlichen Modus (auf allen Domänencontrollern muss W2K ausgeführt werden) befindet!

# Integrierte und vordefinierte Gruppen in einer Domäne:

Integrierte und vordefinierte Gruppen werden bei der Installation von W2K automatisch im Active Directory angelegt. Sie haben eine Reihe von vorbestimmten Rechten und können nicht gelöscht werden. Vordefinierte Gruppen mit einem globalen Bereich befinden sich im Ordner **Users**, die integrierten Gruppen der lokalen Domäne im Ordner **Builtin**.

- Integrierte Gruppen der lokalen Domäne erteilen den Benutzern vordefinierte Rechte und Berechtigungen, um Aufgaben auf Domänencontrollern und im Active Directory auszuführen
- Besondere Identitäten (Sondergruppen) organisieren die Benutzer für die Systemverwendung. Die Mitgliedschaft ist automatisch und kann nicht modifiziert werden.
- Vordefinierte globale Gruppen erteilen den Administratoren die Kontrolle über Domänenressourcen und Benutzer. (im Ordner Users im Active Directory)

# Strategie zum Verwenden von Gruppen in einer Domäne (AGDLP-Strategie):

#### Die AGDLP-Strategie:

- Integrieren von Benutzerkonten (*Accounts* **A**) in einer globalen Gruppe (*Global* **G**) und einbinden dieser Gruppe in Gruppen der lokalen Domäne (Domain Local **DL**)
- Erteilen von Berechtigungen (Permissions P) für die Gruppen der lokale Domäne

# Richtlinien für das Erstellen von Domänengruppen

- Bestimmen des zu verwendenden Gruppenbereichs (globale Gruppen zum Gruppieren von Benutzerkonten und Gruppen der lokalen Domäne für Berechtigungen für eine Ressource)
- Bestimmen der erforderlichen Berechtigungen (nur Mitglieder der Gruppe Administratoren oder Konto-Operatoren verfügen über die Berechtigung zum Erstellen von Gruppen)
- Bestimmen des Gruppennamens

# Erstellen und Löschen von Domänengruppen:

 $Start \rightarrow Programme \rightarrow Verwaltung \rightarrow Computerverwaltung \rightarrow Active Directory-Benutzer und - Computer \rightarrow rechte Maustaste auf Ordner, in der die Gruppe erstellt wird \rightarrow Neu \rightarrow Group$ 

Achtung:	Der Gruppenname (256 Zeichen bei W2k und 20 Zeichen bei WinNT) für die
	Domänengruppe muss eindeutig sein!

Beim Löschen einer Gruppe, werden nur die Rechte und Berechtigungen, welcher zu dieser gehören, nicht aber das Benutzerkonto der Mitglieder gelöscht.

Achtung: Integrierte oder vordefinierte Gruppen können nicht gelöscht werden!

# Hinzufügen von Mitgliedern zu Domänengruppen:

Nach dem Erstellen einer Gruppe können Mitglieder aus Benutzerkonten, andere Gruppen und Computer hinzugefügt werden.

# **Unterrichtseinheit 6**

# NTFS-Berechtigungen:

NTFS-Berechtigungen werden verwendet, um anzugeben, welche Benutzer, Gruppen und Computer auf Dateien und Ordner zugreifen können.

NTFS speichert eine **Zugriffssteuerungsliste** (Access Control List, **ACL**) mit jeder Datei und jedem Ordner auf einer NTFS-Partition. Diese ACL enthält eine Liste aller Benutzerkonten, Gruppen und Computer, denen die Zugriffsberechtigung (und deren Art) für die Datei oder den Ordner erteilt wurde.

Damit ein Benutzer auf eine Datei oder einen Ordner zugreifen kann, muss die ACL einen so genannten **Zugriffssteuerungseintrag** (Access Control Entry, **ACE**) für das Benutzerkonto, die Gruppe oder den Computer, denen der Benutzer angehört, enthalten. (Mit dem DOS-basierten Programm **Cacls.exe** kann man die Berechtigungen für eine Datei, bzw. einen Ordner anzeigen und verändern!)

Achtung:	Wird eine Partition mit NTFS formatiert, so erteilt Windows 2000 der Gruppe
_	Jeder automatisch die Berechtigung Vollzugriff für den Stammordner und
	somit auf alle Ordner und Dateien, die sich darin befinden!

### NTFS-Ordnerberechtigungen:

•	Lesen	Anzeigen der Dateien und Unterordner im Ordner, der Ordnerattribute, der Besitzrechte und der Berechtigungen
•	Schreiben	Erstellen neuer Dateien und Unterordner innerhalb des Ordners, Ändern von Ordnerattributen, sowie Anzeigen der Besitzrechte und Berechtigungen des Ordners
•	Ordnerinhalt auflisten	Anzeigen der Namen von Dateien und Unterordnern im Ordner
•	Lesen, Ausführen	Durchsuchen der Ordner und Ausführen von Aktionen, die von den Berechtigungen <b>Lesen</b> und <b>Ordnerinhalt</b> <b>auflisten</b> zugelassen werden
•	Ändern	Löschen des Ordners und Ausführen von Aktionen, die von den Berechtigungen <b>Schreiben</b> und <b>Lesen, Ausführen</b> zugelassen werden
•	Vollzugriff	Änderungen von Berechtigungen, Übernehmen von Besitzrechten, Löschen von Unterordnern und Dateien, sowie Ausführen von Aktionen, die von allen anderen NTFS- Ordnerberechtigungen zugelassen werden

### NTFS-Dateiberechtigungen:

Lesen der Datei und Anzeigen der Dateiattribute, der

Besitzrechte und der Berechtigungen

• **Schreiben** Überschreiben der Datei, Ändern der Dateiattribute,

sowie Anzeigen der Besitzrechte und Berechtigungen

der Datei

• Lesen, Ausführen Ausführen von Anwendungen und Aktionen, die von der

Berechtigung **Lesen** zugelassen werden

• Ändern und Löschen der Datei, sowie Ausführen von

Aktionen, die von den Berechtigungen Schreiben und

Lesen, Ausführen zugelassen werden

• Vollzugriff Ändern von Berechtigungen, Übernehmen von Besitz-

rechten, sowie Ausführen der Aktionen, die von allen anderen NTFS-Dateiberechtigungen zugelassen werden

# Mehrfache NTFS-Berechtigungen:

NTFS-Berechtigungen sind kumulativ, d.h. sie setzen sich aus einer Kombination der Berechtigungen der einzelnen Benutzer und der Gruppen, denen sie angehören zusammen.

NTFS-Dateiberechtigungen haben allerdings Vorrang vor NTFS-Ordnerberechtigungen und setzen diese somit außer Kraft.

**Achtung:** Eine Ausnahme bildet die Berechtigung **Verweigern**, die alle anderen Berechtigungen (egal, woher diese zugeordnet sind) außer Kraft setzt.

# Vererbung von NTFS-Berechtigungen:

Alle Berechtigungen, die für einen Ordner erteilt werden, gelten automatisch auch für alle darin vorhandenen und neu hinzugefügten Unterordner und Dateien.

Diese Vererbung kann unterbrochen werden, indem einem Unterordner neue Berechtigungen zugeteilt und diese wiederum nach unten weitergegeben werden.

Wird ein Ordner oder eine Datei innerhalb einer oder zwischen einzelnen NTFS-Partitionen kopiert, so erbt diese Kopie die Berechtigungen des Zielordners.

Ein Verschieben eines Ordners oder einer Datei **innerhalb einer NTFS-Partition** bewirkt ein beibehalten der ursprünglichen Berechtigungen, wohingegen beim Verschieben **zwischen einzelnen NTFS-Partitionen** die Berechtigungen des Zielordners übernommen werden. (Es müssen beim Verschieben die Berechtigungen **Schreiben** für den Zielordner und **Ändern** für den Quellordner verfügbar sein!)

Wird ein Ordner oder eine Datei von einer NTFS-Partition auf eine Nicht-NTFS-Partition kopiert oder verschoben, so verlieren diese alle Berechtigungen, da nur NTFS-Dateisysteme eine Vergabe von Rechten unterstützen.

# Erteilen von NTFS-Berechtigungen:

Administratoren, Benutzer mit der Berechtigung **Vollzugriff**, sowie Besitzer von Dateien oder Ordnern können Benutzerkonten und Gruppen Berechtigungen für diese erteilen.

(Rechte Maustaste auf den Ordner oder die Datei, für welche Berechtigungen erteilt werden sollen → Eigenschaften → Sicherheitseinstellungen)

## Optimale Methoden zum Erteilen von NTFS-Berechtigungen:

- Berechtigungen nur den Gruppen, nicht aber den Benutzern erteilen (Steigerung der System-Leistung)
- Um die Verwaltung zu vereinfachen, sollten Ressourcen auf einer separaten Partition gruppiert werden
- Dem Benutzer nur die Zugriffsebene, welche er benötigt gewähren
- Gruppen werden gemäß dem Zugriff für die Ressourcen, den die Gruppenmitglieder benötigen, erstellt
- Anwendungsordner sollten für die Gruppe Benutzer und Administratoren nur die Berechtigung Lesen, Ausführen erhalten, um ungewollten Datenverlust (auch durch Viren) zu verhindern
- Datenordner sollten für die Gruppe Benutzer die Berechtigungen Lesen, Ausführen und Schreiben erhalten, der Besitzer Vollzugriff

# Erteilen spezieller NTFS-Berechtigungen:

Damit ein Benutzer einem Administrator die Möglichkeit zum Ändern von Berechtigungen auf seine Ordner oder Dateien geben kann, muss er der Gruppe **Administratoren** die Berechtigung **Berechtigungen ändern** für diese erteilen.

Besitzrechte können von einem Benutzerkonto, bzw. einer Gruppe auf ein anderes Benutzerkonto, bzw. Gruppe übertragen werden. Die Vorraussetzung dafür ist der Vollzugriff auf den entsprechenden Ordner, bzw. Datei. Somit kann ein Mitglied der Gruppe **Administratoren** auch dann Besitzrechte für einen Ordner, bzw. Datei übernehmen, wenn ihm keine Berechtigungen dafür erteilt wurden.

(Rechte Maustaste auf den Ordner oder die Datei, für welche Berechtigungen erteilt werden sollen  $\rightarrow$  Eigenschaften  $\rightarrow$  Sicherheitseinstellungen  $\rightarrow$  Erweitert  $\rightarrow$  auf das entsprechende Benutzerkonto/Gruppe klicken  $\rightarrow$  Anzeigen/Bearbeiten)

# Komprimieren von Daten auf einer NTFS-Partition:

Alle Dateien und Ordner auf einer NTFS-Partition haben einen Komprimierungsstatus, der entweder komprimiert oder unkomprimiert ist.

Beim Arbeiten mit komprimierten Dateien sollten jedoch folgende Aspekte berücksichtigt werden:

- Speicherplatzreservierung (NTFS reserviert Speicherplatz basierend auf der Größe der **unkomprimierten** Datei)
- Anzeigefarbe für den Komprimierungsstatus (die Farben, in der komprimierte Dateien und Ordner angezeigt werden, können geändert werden)
- Zugriff auf komprimierte Dateien über Anwendungen (alle MS-basierten Anwendungen können komprimierte Dateien lesen und schreiben, ohne dass die Dateien zuerst dekomprimiert werden müssen)

Mit Hilfe des Windows Explorers kann der Komprimierungsstatus festgelegt und die Anzeigefarbe für komprimierte Dateien und Ordner geändert werden.

Achtung: Verschlüsselte Ordner und Dateien können nicht komprimiert werden!

# Festlegen des Komprimierungsstatus:

(Rechte Maustaste auf den Ordner oder die Datei, für welche die Komprimierung erteilt werden soll  $\rightarrow$  Eigenschaften  $\rightarrow$  Erweitert...  $\rightarrow$  Inhalt komprimieren, um Speicherplatz zu sparen)

Wird ein Ordner komprimiert, zeigt W2K zusätzlich das Dialogfeld Änderungen der Attribute bestätigen, indem festgelegt wird, ob sich die Komprimierung nur auf diesen Ordner, oder auch auf alle Unterordner bezieht, an.

Die Anzeigefarbe für komprimierte Dateien und Ordner kann im Windows Explorer unter  $Extras \rightarrow Ordneroptionen \rightarrow Ansicht \rightarrow Komprimierte Dateien und Ordner in anderer Farbe anzeigen eingestellt werden.$ 

# Kopieren und Verschieben von komprimierten Dateien und Ordnern:

- Wird eine Datei oder ein Ordner **innerhalb einer NTFS-Partition** kopiert, so erbt diese(r) den Komprimierungsstatus des Zielordners.
- Wird eine Datei oder ein Ordner **innerhalb einer NTFS-Partition** verschoben, so behält diese(r) den ursprünglichen Komprimierungsstatus bei.
- Wird eine Datei oder ein Ordner **zwischen NTFS-Partitionen** kopiert oder verschoben, so erbt diese(r) den Komprimierungsstatus des Zielordners.

Achtung: Windows 2000 unterstützt Komprimierung nur für NTFS-Partitionen! Wird eine komprimierte Datei oder Ordner auf einen Nicht-NTFS-Datenträger verschoben oder kopiert, so wird diese(r) automatisch dekomprimiert.

Wird eine komprimierte Datei kopiert, so wird diese erst dekomprimiert, danach kopiert und anschließend wieder komprimiert. Dies kann Leistungseinbußen verursachen.

# Optimale Methoden zum Komprimieren von Daten:

- Bestimmung der Dateitypen, welche komprimiert werden sollen
- Keine bereits komprimierten Dateien komprimieren
- Verwendung anderer Anzeigefarben f
   ür komprimierte Dateien und Ordner
- Komprimierung statischer, anstelle von sich häufig ändernden Dateien (Steigerung der Systemleistung)

# Konfigurieren von Datenträgerkontingenten auf NTFS-Partitionen:

Datenträgerkontingente (nur auf NTFS-Dateisystemen: NTFS5) werden zum Verwalten der wachsenden Speichermenge (beschränken von Speicherplatz für Benutzer) in verteilten Umgebungen eingesetzt.

(Rechte Maustaste auf den Datenträger, für welchen die Beschränkung erteilt werden soll → Eigenschaften → Kontingent → Kontingentenverwaltung aktivieren)

- Die Berechnung der Speicherplatzverwendung basiert auf Datei- und Ordnerbesitzrechten (unabhängig vom Speicherort – nur vom Benutzeraccount)
- Datenträgerkontingente verwenden keine Datenträgerkomprimierung, daher wird die Komprimierung bei der Berechnung der Speicherplatzverwendung ignoriert
- Der freie Speicherplatz für Anwendungen basiert auf der Kontingentbeschränkung
- Datenträgerkontingente werden für jede NTFS-Partition getrennt überwacht, auch wenn sich die Partitionen auf derselben physischen Festplatte befinden

# Schützen von Daten mit Hilfe von EFS (standardmäßig 64Bit):

Das verschlüsselnde Dateisystem EFS (Encrypting File System) stellt Verschlüsselung für NTFS-Dateien auf Dateiebene bereit und ermöglicht somit den Benutzern das Speichern von Daten auf der Festplatte im verschlüsselten Format.

- EFS wird im Hintergrund ausgeführt (für Benutzer und Anwender transparent)
- Es ermöglicht nur autorisierten Benutzern den Zugriff auf eine verschlüsselte Datei
- Es stellt integrierte Unterstützung für Datenwiederherstellung bereit (Dateiverschlüsselung kann allerdings nur dann verwendet werden, wenn der lokale Computer mit einem oder mehreren Wiederherstellungsschlüsseln konfiguriert ist)
- Es erfordert mindestens einen Wiederherstellungs-Agenten zum Wiederherstellen verschlüsselter Dateien

Achtung: Verschlüsselung und Komprimierung schließen sich gegenseitig aus!

## Verschlüsseln eines Ordners oder einer Datei:

(Rechte Maustaste auf den Ordner, für welchen die Verschlüsselung aktiviert werden soll → Eigenschaften → Erweitert... → Inhalt verschlüsseln, um Daten zu schützen aktivieren)

Ist ein Ordner verschlüsselt, so werden alle in ihm gespeicherten Dateien und Unterordner automatisch mit Hilfe von Dateiverschlüsselungsschlüsseln verschlüsselt. Beim Verschieben der verschlüsselten Datei, bzw. Ordner auf der gleichen Partition, bleibt die Verschlüsselung erhalten.

Der Zugriff auf die verschlüsselte Datei wird allen Benutzern, mit Ausnahme des Besitzers des privaten Schlüssels (oder des Wiederherstellungs-Agenten mit Hilfe des eigenen privaten Schlüssels), verweigert. (Eine verschlüsselte Datei kann nicht mit anderen Benutzern gemeinsam genutzt werden)

# Wiederherstellen eines verschlüsselten Ordners, bzw. Datei:

Um als Wiederherstellungs-Agent eine verschlüsselte Datei oder einen verschlüsselten Ordner mit Hilfe des Windows-Programms **Sicherung** wieder herzustellen, sollte sich dieser an der lokalen Workstation des Benutzers, welcher die Datei, bzw. den Ordner verschlüsselt hat, befinden.

(Rechte Maustaste auf den Ordner, für welchen die Entschlüsselung aktiviert werden soll → Eigenschaften → Erweitert... → Inhalt verschlüsseln, um Daten zu schützen deaktivieren)

Aktivieren der Management Console (MMC):

#### **Export des Generalschlüssels:**

 $(Start \rightarrow Ausführen \rightarrow MMC \rightarrow Konsole \rightarrow Snap-In hinzufügen/entfernen \rightarrow Hinzufügen \rightarrow Zertifikate \rightarrow speichern \rightarrow Zertifikate aktueller Benutzer \rightarrow eigene Zertifikate \rightarrow Zertifikate \rightarrow mit rechter Maustaste auf den Benutzer klicken <math>\rightarrow$  alle Tasks  $\rightarrow$  exportieren)

#### **Import des Generalschlüssels:**

(Gespeicherte Management Console starten → Zertifikate aktueller Benutzer → eigene Zertifikate → Zertifikate → mit rechter Maustaste auf den Benutzer klicken → alle Tasks → importieren)

# **Unterrichtseinheit 7**

## Freigegebene Ordner:

Durch freigegebene Ordnern können Benutzer Zugriff auf Dateien und Ordner innerhalb eines Netzwerkes (auch bei verstreut gespeicherten Daten, mit Hilfe des Distributed File System [DFS] – verteiltes Dateisystem) erhalten. Diese Ordner können Anwendungen, Dateien oder persönliche Daten eines Benutzers beinhalten. Durch freigegebene Ordner kann die Administration und die Sicherung von Daten innerhalb eines Netzwerkes, durch zentralisierte Verwaltung, vereinfacht werden.

## Erstellen freigegebener Ordner:

Ein Benutzer kann einen Ordner nur dann freigeben, wenn er für den Computertyp, auf dem sich dieser Ordner befindet, die Freigabe-Berechtigung besitzt.

Eine Steuerung über den Zugriff auf freigegebene Ordner und dessen Inhalt kann über dessen Eigenschaften, ausgewählten Benutzer oder Gruppen und die maximale Anzahl der gleichzeitigen User begrenzt werden.

## Anforderung für das Freigeben von Ordnern

In Windows 2000 können Ordner nur von Mitgliedern der Gruppe *Administratoren*, *Server-Operatoren* (Windows2000-Domäne) und *Hauptbenutzer* (Windows2000-Arbeitsgruppe) freigegeben werden.

Anforderungen für das Freigeben von Ordner:

- Der Ordner muss sich auf einem Computer befinden, der Teil einer Domäne oder Arbeitsgruppe ist
- Das Betriebssystem muss die Freigabe von Ordnern unterstützten

# Freigeben eines Ordners

Wird ein Ordner (einmal oder mehrmals) freigegeben, muss diesem erst ein Freigabename zugewiesen und anschließend dessen Beschränkungen, bzw. Eigenschaften konfiguriert werden.

Explorer → Rechte Maustaste auf den freizugebenden Ordner → Freigabe

#### Folgende Optionen können konfiguriert werden:

**Diesen Ordner freigeben** Option um den Ordner freizugeben

Freigabename Name des freigegebenen Ordners, der im Netzwerk

angezeigt wird. (Standardmäßig wird der Ordnername

verwendet)

**Kommentar** Beschreibung des freizugebenden Ordners

**Benutzerbegrenzung** Anzahl der Benutzer, die gleichzeitig zugreifen können

(max. bis zu 10 Verbindungen)

**Berechtigungen** hier werden die Berechtigungen für den freizugebenden

Ordner verwaltet

## Berechtigungen

Benutzer (Benutzerkonten, Gruppen oder Computerkonten), die über das Netzwerk zugreifen, können Berechtigungen (gelten für den freigegebenen Ordner, nicht aber für die Dateien) erteilt oder verweigert werden. Diese haben jedoch keinen Einfluss auf die lokalen Zugriffs-Berechtigungen des Computers.

### Folgende Berechtigungen können eingestellt werden:

Lesen Anzeigen von Ordnernamen, Dateidaten und

Dateiattributen, ausführen von Anwendungen und Ändern von

Ordnern innerhalb des freigegebenen Ordners.

Ändern Erstellen von Ordnern, Hinzufügen von Dateien zu Ordnern,

Ändern von Daten in Dateien und Dateiattributen, anhängen von Daten an Dateien, Löschen von Ordner und Dateien und alle

Aktionen, die durch Berechtigung **Lesen** zugelassen sind.

Vollzugriff Ändern von Dateiberechtigungen, übernehmen des Besitzes und

alle Aktionen, die durch die Berechtigungen Ändern und Lesen

zugelassen sind.

Achtung: Standardmäßig verfügen alle Benutzer über die Berechtigung Vollzugriff

für einen freigegebenen Ordner. Um nur einigen Benutzern den Berechtigungen zu erteilen, muss die Gruppe **Jeder** entfernt werden.

(Wird die Berechtigung der Gruppe Jeder auf verweigern gesetzt, wird

**allen** Benutzern der Zugriff entzogen!)

Tatsächliche Berechtigungen eines Benutzers ergeben sich durch dessen Berechtigung auf den freigegebenen Ordner und die Berechtigung der Gruppe in der er sich befindet, wobei immer die höhere Berechtigung ausschlaggebend ist.

Berechtigungen können auch verweigert werden. Dies setzt alle anderen Berechtigungen außer Kraft.

Zum Zuweisen der Rechte und Berechtigungen sollte die Gruppe **Authentifizierte Benutzer** (statt der Gruppe **Jeder**) verwendet werden, da auf diese Weise das Risiko eines nicht autorisierten Zugriffs minimiert wird.

Möchte ein Benutzer auf einen freigegebenen Ordner, welcher sich auf einem NTFS-Datenträger befindet, zugreifen, so benötigt er, ergänzend zu den Berechtigungen dieses Ordner, für jede Datei und jeden darin liegenden Ordner zudem noch die entsprechende NTFS-Berechtigung.

**Achtung:** Die Freigabe funktioniert mit allen Dateisystemen, die Sicherheit allerdings nur mit NTFS!

# Mehrfaches Freigeben eines Ordners:

Um einen Ordner mehrfach freizugeben, muss der Ordner bereits unter einem Namen freigegeben sein.

Explorer  $\rightarrow$  Rechte Maustaste auf den freizugebenden Ordner  $\rightarrow$  Freigabe  $\rightarrow$  Neuer Freigabenamen für den Ordner eingeben

Wird die Freigabe eines Ordners aufgehoben, während ein Benutzer eine Datei aus diesem geöffnet hat, so verliert dieser möglicherweise Daten. Um dies zu verhindern, ist in Windows 2000 eine Sicherheit in Form eines Dialogfeldes eingebaut, das Informationen darüber gibt, das Benutzer (während des Aufhebens der Freigabe) noch mit diesem Ordner verbunden sind.

# Herstellen einer Verbindung zu freigegeben Ordnern

Nachdem ein Ordner freigegeben wurde, können Benutzer über das Netzwerk darauf zugreifen.

Um den Zugriff auf einen freigegebenen Ordner eines anderen Computers zu erhalten, kann die Verbindung mit Hilfe von **Netzwerkumgebung**, **Netzlaufwerk verbinden** (hier können freigegebene Ordner als virtuelles Laufwerk dargestellt werden und müssen nicht über einen umständlichen Weg geöffnet werden) oder **Ausführen** (hier ist kein Laufwerksbuchstabe notwendig, dadurch kann man damit eine unbegrenzte Anzahl an Verbindungen herstellen) erstellt werden.

# Kombinieren von NTFS-Berechtigungen und Berechtigungen für freigegebene Ordner

Eine Strategie, um den Zugriff auf Netzwerkressourcen auf einer NTFS-Partition zu steuern besteht darin, Ordner mit den Standardberechtigungen für freigegebene Ordner freizugeben und anschließend den Zugriff auf diese Ordner durch das erteilen von NTFS-Berechtigungen zu steuern.

Wird ein Ordner auf einer NTFS-Partition freigegeben, so werden die Berechtigung für freigegebene Ordner und die NTFS-Berechtigung (unabhängig davon, ob ein lokal-, oder ein Netzwerkzugriff erfolgt) kombiniert, um Dateiressourcen zu schützen.

### Es gelten folgende Regeln:

- Auf NTFS-Datenträgern sind NTFS-Berechtigungen erforderlich
- Benutzer benötigen NTFS-Berechtigungen und Berechtigungen für den freigegebenen Ordner
- Es gilt immer die restriktivste (höchste) Kombination der Berechtigungen für freigegebene Ordner und NTFS-Berechtigungen

# Verwenden von administrativen freigegebenen Ordnern

2000 gibt automatisch Ordner, welche das Ausführen Windows Verwaltungsaufgaben für Administratoren (Vollzugriff) ermöglichen und für normale Benutzer ausgeblendet sind, frei.

C\$, D\$, E\$ Admin\$ Print\$

der Stamm jeder Partition wird automatisch freigegeben der Ordner C:\Winnt wird als Admin\$ freigegeben

der Ordner mit den Druckertreibern (beim Erstellen des ersten Druckers - %SystemRoot%\System32\Spool\Drivers) wird als

**Print\$** freigegeben

# Veröffentlichen eines freigegebenen Ordners in Active Directory

Durch das Veröffentlichen von Ressourcen, einschließlich freigegebener Ordner (mit UNC-Namen), in Active Directory wird es Benutzern ermöglicht, dieses zu durchsuchen und Ressourcen im Netzwerk auch dann zu finden, wenn der physische Speicherort der Ressourcen (muss allerdings aktualisiert werden) geändert wurde.

Um einen freigegebenen Ordner in Active Directory zu veröffentlichen, müssen folgende Schritte ausgeführt werden:

Start → Programme → Verwaltung → Active Directory-Benutzer und -Computer → rechte Maustaste auf die Domäne mit den freizugebenden Ordner → Neu → Shared Folder → Name und Netzwerkpfad eingeben

# Einführung in DFS (Distributed File System)

DFS ist ein Dienst, der einen einzelnen Zugriffspunkt und eine logische Verzeichnisstruktur für Dateiressourcen bereitstellt, deren physische Speicherorte über das gesamte Netzwerk verteilt sein können.

• Organisieren von Ressourcen DFS verwendet eine Verzeichnisstruktur, die einen Stamm - welcher mehrere Verknüpfungen enthalten kann, von denen jede auf freigegebene Ordner verweist - und DFS-Verknüpfungen enthält.

Vereinfachen der Navigation

Nachdem eine Verbindung zu einem DFS-Stamm hergestellt wurde, können Benutzer alle untergeordneten Ressourcen durchsuchen und darauf unabhängig vom physischen Standort des Servers zugreifen

Vereinfachen der Verwaltung

Bei einem Serverausfall kann der Speicherort der freigegebenen Ordners von einem Server auf einen anderen Server verschoben werden, ohne das Benutzer (welche weiterhin denselben Pfad für die Verknüpfung verwenden) diese Änderung bemerken.

### Beibehalten von Berechtigungen

Ein Benutzer kann über DFS nur auf einen freigegebenen Ordner zugreifen, wenn er bei diesem über die geeigneten Zugriffsrechte verfügt.

Achtung:	Nur Clientcomputer mit DFS-Clientsoftware können Zugriff auf
	DFS Ressourcen erhalten. Nur für Windows 95 muss eine
	dementsprechende Software downgeloaded werden, alle
	anderen Systeme (98/2000/NT4.0) schließen diese ein.

### Arten von DFS-Stämmen

Ein DFS-Stamm, sowohl auf Domänen-, als auch auf Serverebene, ist die oberste Ebene der DFS-Topologie.

#### 1. Eigenständiger DFS-Stamm

- Ist auf einem einzelnen Computer gespeichert
- Verwendet nicht Active Directory
- Kann keine freigegebenen Ordner auf der DFS-Stammebene enthalten
- Unterstützt nur eine einzige Ebene von DFS-Verknüpfungen

#### 2. <u>Domänenbasierter DFS-Stamm</u>

- Mehrere Domänencontroller oder Mitgliedsserver dienen als Host
- DFS-Topologie ist in Active Directory gespeichert
- Kann freigegebene Ordner auf der DFS-Stammebene enthalten
- Unterstützt mehrere Ebenen mit DFS-Verknüpfungen

# Zugreifen auf Dateiressourcen über DFS

Obwohl eine DFS-Hierarchie wie eine gewöhnliche Ordnerhierarchie im Explorer angezeigt wird, besteht der Unterschied darin, dass DFS den Benutzern einen einzelnen Zugriffspunkt für Ressourcen, welche sich an unterschiedlichen physischen Speicherorten befinden können, zur Verfügung stellt.

Wird auf eine DFS-Verknüpfung zugegriffen, geschieht folgendes:

- 1. Client stellt eine Verbindung zum DFS-Host-Server her (nur beim ersten Mal)
- 2. Client erhält vom Host einen Verweis auf die DFS-Verknüpfung (nur beim ersten Mal)
- 3. DFS-Client stellt eine Verbindung zur DFS-Verknüpfung her, auf dem sich der freigegebene Ordner befindet und speichert diesen Verweis zwischen. In regelmäßigen Abständen stellt der DFS-Client eine Verbindung zum Host-Server her, um den Verweis zu aktualisieren.

Achtung:	DFS verwendet für seine Verknüpfungen keine separaten NTFS-
_	Berechtigungen, bzw. Berechtigungen für freigegebene Ordner!

# Erstellen eines DFS-Stammes

Start → Programme → Verwaltung → Verteiltes Dateisystem (DFS) → Vorgang → Neuen DFS-Stamm

#### Konfigurieren des DFS-Stammes

- DFS-Typ auswählen (Domänen- oder eigenständigen DFS-Stamm)
- Hostdomäne für DFS-Stamm oder Hostserver auswählen
- Freigabe für den DFS-Stammdatenträger angeben
- Name des DFS-Stamms

## Hinzufügen von DFS-Verknüpfungen

 $Start \rightarrow Programme \rightarrow Verwaltung \rightarrow Verteiltes Dateisystem (DFS) \rightarrow DFS-Stamm auswählen \rightarrow Vorgang \rightarrow Neue DFS-Verknüpfung$ 

### Konfigurieren der "neuen DFS-Verknüpfung"

- Verknüpfungsname
- Benutzer zu diesem freigegebenen Ordner senden
- Kommentar
- Clients speichern diese Referenz x Sekunden zwischen

## Replikate für die Fehlertoleranz

Start  $\rightarrow$  Programme  $\rightarrow$  Verwaltung  $\rightarrow$  Verteiltes Dateisystem (DFS)  $\rightarrow$  DFS-Verknüpfung auswählen  $\rightarrow$  Neues Replikat  $\rightarrow$  Automatische/Manuelle Replikation

Replikate, eine weitere Instanz einer DFS-Verknüpfung, ermöglichen Fehlertoleranz und Lastenausgleich. Auf mindestens einem anderen Server befindet sich eine Kopie einer DFS-Verknüpfung. Durch Replikate stellen beim Ausfall des Hostcomputers die Clientcomputer automatisch eine Verbindung zu diesem her.

Wichtig: Jede DFS-Verknüpfung kann bis zu 32 Replikate besitzen.

# Konfigurieren der Replikation

Bei mehreren Replikationen muss immer sichergestellt werden, dass alle Kopien die gleichen Daten enthalten. (Synchronisation)

Mit Hilfe des Fensters **Replikationsrichtlinie** der DFS-Konsole kann die automatische Replikation aktiviert werden. Um eine Replikationsrichtlinie festzulegen, wird einer der freigegebenen DFS-Ordner als erster Master (Masterkopie) ausgewählt und dessen Inhalt dann anschließend an die anderen freigegebenen DFS-Ordner in deren Gruppe repliziert. Diese Replikation erfolgt im Rahmen der Active Directory-Replikation.

### Durch eine Statusprüfung können folgende Ergebnisse ausgewertet werden:

- o Replikat wurde gefunden → Zugriff auf das Replikat ist möglich
- Replikat wurde gefunden → Zugriff auf das Replikat nicht möglich (evtl. fehlende NTFS-Berechtigung)
- o Replikat nicht gefunden → freigegebener Ordner ist nicht verfügbar

# **Unterrichtseinheit 8**

# Überwachen von Ereignisprotokollen:

Ereignisse werden überwacht, um Sicherheitsereignisse, die Ressourcenverwaltung oder System- und Anwendungsfehler identifizieren und nachverfolgen zu können. Systemereignisse werden von Windows 2000 automatisch konfiguriert und im Systemprotokoll aufgezeichnet, wohingegen Anwenderereignisse vom Anwendungsentwickler bestimmt und im Anwendungsprotokoll aufgezeichnet werden.

 $Start \rightarrow Programme \rightarrow Verwaltung \rightarrow Ereignisanzeige$ 

# Einführung in Ereignisprotokolle

Ereignisprotokolle ermöglichen die Überwachung von Hard- und Software, Systemproblemen und Sicherheit.

Es existieren drei Arten von Protokollen:

•	<u>Systemprotokoll</u>	enthält	die	von	Windows	2000	VOI	rherbestim	ım-
		ten pro	tokol	lierter	n Ereignist	ypen (	der	Systemko	m-
		ponente	n.						

Anwendungsprotokoll enthält von Anwendungen oder Programmen proto-

kollierte Ereignisse. Der Programmentwickler entscheidet, welche Ereignisse aufgezeichnet werden.

• <u>Sicherheitsprotokoll</u> Sicherheitsereignisse werden im Zusammenhang

mit Anmeldeversuchen und der Ressourcenverwendung aufgezeichnet. Welche Ereignisse im Sicherheitsprotokoll aufgezeichnet werden sollen,

legt der Administrator fest.

Achtung: Anwendungs- und Systemprotokolle können von allen Benutzern angezeigt werden, während auf Sicherheitsprotokolle nur Systemadministratoren zugreifen können.

Arten von System- und Anwendungsereignissen

Es gibt drei Arten von System- und Anwendungsereignissen:

- <u>Information</u> Die erfolgreiche Ausführung einer Anwendung, eines Treibers oder eines Dienstes
- Warnung
   Ein Ereignis, das nicht notwendigerweise bedeutsam ist, aber möglicherweise auf ein zukünftiges Problem bei Systemvorgängen hinweist.
- <u>Fehler</u> Ein bedeutsames Problem bei Systemvorgängen, wie z.B. ein Daten- oder Funktionalitätsverlust.

# Anzeigen von Ereignisprotokollen

System- und Anwendungsereignisse werden in den zugeordneten Protokolldateien sequenziell protokolliert.

Zusätzlich zum Anzeigen eines lokalen Protokolls, kann auch ein Protokoll für einen Remotecomputer angezeigt werden. (In der **Ereignisanzeige** mit der rechten Maustaste klicken und **Verbindung zu anderem Computer herstellen** auswählen)

**Achtung:** Ein Domänencontroller verfügt über mehr als diese drei Protokolle!

Man kann auch nach bestimmten Ereignissen, bzw. nach einer Gruppe von Ereignissen suchen ( $Start \rightarrow Programme \rightarrow Verwaltung \rightarrow Ereignisanzeige \rightarrow Ansicht \rightarrow Suchen$ ).

Um die Filterfunktion zum Suchen zu aktivieren, muss man mit der rechten Maustaste auf Sicherheits-, System- oder Anwendungsprotokoll, dann auf Ansicht und anschließend auf Filter klicken.

## Beschränkung von Protokolldateigrößen

Ereignisprotokolle können, um Speicherplatzproblemen auf der Festplatte vorzubeugen, durch überschreiben älterer Ereignisprotokolle beschränkt werden. Um Protokolldateien zu konfigurieren, muss man das entsprechende Protokoll in der Ereignisanzeige auswählen. Hier stehen folgende Optionen zur Verfügung:

- Ereignisse nach Bedarf überschreiben diese Einstellung erfordert keine Verwaltung und kann bei niedriger Sicherheit gewählt werden – Überprüfung täglich
- Ereignisse überschreiben die älter als x Tage sind diese Einstellung sollte man wählen, wenn die Überprüfung alle drei bis fünf Tage erfolgt
- Ereignisse nie überschreiben [Protokoll manuell löschen]
  hier muss das Löschen des Protokolls manuell erfolgen. Wenn dieses voll ist,
  zeichnet W2k keine weiteren Ereignisse mehr auf. Diese Einstellung sollte bei
  sehr hoher Sicherheit ausgewählt werden. W2k kann auch so konfiguriert
  werden, dass ein volles Sicherheitsprotokoll zum Herunterfahren des Systems
  führt.

# Verwalten von Ereignisprotokollen

- 1. <u>Die Ereignisprotokolle sollten für folgende Zwecke archiviert werden:</u>
  - zum Nachverfolgen von Trends, um die Ressourcenverwendung zu bestimmen
  - zum Nachverfolgen nicht autorisierter Ressourcenverwendung
  - zum Aufbewahren von Aufzeichnungen aus rechtlichen Gründen

### 2. Folgende Dateiformate zum Anzeigen archivierter Protokolle sind möglich:

- 1. Protokolldateiformat (EVT)
- 2. Textdateiformat (TXT)
- 3. Textdateiformat mit Kommas als Trennzeichen (CSV)
- 3. Löschen der Ereignisprotokolle, wenn diese nicht überschrieben werden sollen

# Verwenden des Task-Managers

Der Task-Manager stellt Echtzeitinformationen über derzeit auf dem System ausgeführte Anwendungen, Prozessen und ihrer Speicherverwendung (ein Programm, welches in einem reservierten Arbeitsspeicherbereich ausgeführt wird) oder anderen Prozessdaten, sowie zu Statistiken über die Arbeitsspeicher- und Prozessorleistung bereit.

### 1. Überwachen von Programmen

Mit der Registerkarte **Anwendungen** kann der Status (**wird ausgeführt** oder **keine Rückmeldung** – kann über **Task beenden** beendet werden) aller ausgeführten Anwendungen überwacht werden.

Um den zugeordneten Prozess einer Anwendung zu identifizieren, muss man mit der rechten Maustaste erst auf die Anwendung und dann auf **Zum Prozess wechseln** klicken, worauf die Registerkarte **Prozesse** mit dem zugeordneten Prozess angezeigt wird.

### 2. Überwachen von Prozessen

In der Registerkarte **Prozesse** werden alle ausgeführten Prozesse und Ihre Maße (quantitative Angaben eines Prozesses, wie CPU-Nutzung[%], CPU-Zeit, Speichernutzung, E/A [Lesen], E/A [Schreiben]) angezeigt.

Zum Anzeigen anderer Eigenschaften muss auf **Ansicht** und anschließend auf **Spalten auswählen** geklickt werden.

# 3. Überwachen der Leistung

Zum Überwachen der aktuellen (dynamischen prozessor- und speicherverwendenden) Leistungen wird die Registerkarte Systemleistung verwendet.

# Verwenden des Systemmonitors zum Überwachen der Systemleistung

Um ausführlichere Details des Computers und dessen Leistung zu erhalten wird der Systemmonitor ( $Start \rightarrow Programme \rightarrow Verwaltung \rightarrow Systemmonitor$ ) verwendet.

Objekte: Im Systemmonitor sind Objekte (Hardware und Software) wichtige Komponenten oder Subsysteme des Computersystems

**Achtung:** Systemmonitorobjekte sind nicht das Gleiche wie Objekte von Active Directory und haben nichts mit diesen zu tun!

Instanzen: dies sind mehrere Exemplare desselben Objekttyps

sammeln Daten zu verschiedenen Aspekten von Leistungsindikatoren:

Objekten. Im Systemmonitor wird angeben, welche

Leistungsindikatoren angezeigt werden sollen.

# Anzeigen der Leistungsindikatoren

Die Daten können auf drei Arten in Echtzeit angezeigt werden:

1. Histogramm zeigt Daten in einem Balkendiagramm an

2. Bericht zeigt numerische Daten in Spalten an (zum weiterverar-

beiten in Tabellenkalkulationsprogrammen)

zeigt Daten in einem Kurvendiagramm an 3. **Diagramm** 

Auch mit dem Tool Leistungsdatenprotokolle können Daten in Echtzeit angezeigt werden. Es gibt dabei zwei Arten von Protokollen:

 Leistungsindikatorenprotokolle: (dauernde kontinuierliche Darstellung)

> zeichnen Daten zu Hardwareressourund Systemdiensten auf der Grundlage der Leistung über längere

Zeiträume auf

• Protokolle der Ablaufverfolgung: (wird erst ab dem Eintreten des Ereig-

> nisses aktiv) sammeln Ablaufverfolgungen mit Leistungsstatikmaßen zu Ereignissen, wie z.B. Datenträger- und

Datei-E/A-Ereignissen

# Verwenden von Warnungen

Warnungen werden zum Benachrichtigen eines Benutzers oder Administrators beim Überschreiten festgelegter Kriterien (bestimmte Leistungsindikatoren, welche nicht aktiv überwacht werden) verwendet.

Man kann Warnungen so konfigurieren, dass diese eine Netzwerkmeldung sendet, ein Programm ausführt oder ein Protokoll startet.

Zum Ausführen des Tools Leistungsdatenprotokolle und Warnungen muss man über Administratorrechte verfügen.

#### Warnungen werden wie folgt festgelegt:

Start → Programme  $\rightarrow$ Verwaltung Systemmonitor → **Leistungsdatenprotokolle und Warnungen** → Warnungen → rechte Maustaste auf **Neue Warnungseinstellungen**  $\rightarrow$  Namen vergeben  $\rightarrow$  auf der Registerkarte **Allgemein** einen Kommentar mit einer Kurzbeschreibung vergeben  $\rightarrow$ Hinzufügen → hier die entsprechenden Leistungsindikatoren auswählen und auf der Registerkarte Allgemein die Eigenschaften für das Abtastintervall und den Warnschwellenwert festlegen  $\rightarrow$  Auf der Registerkarte Vorgang Kontrollkästchen Einen Eintrag im Ereignisprotokoll der Anwendungen protokollieren aktivieren → auf der Registerkarte Zeitplan unter Suche starten und **Suche beenden** die Parameter festlegen → **OK** 

## Optimieren der Leistung

Um das Betriebssystem und die Anwendungen die Systemressourcen effizienter verwenden zu können, sollte die Leistung (Basislinie) des Computers optimiert werden.

Zu den wichtigsten Ressourcen, welche überwacht werden sollten, um die Basislinie beizubehalten, gehören folgende:

- Arbeitsspeicher
- Prozessor
- Datenträgeraktivität
- Netzwerkaktivität

## Prozess der Leistungsoptimierung

Durch die Optimierungsprozesse kann bestimmt werden, welche Aktionen zum Verbessern der Systemleistung – entsprechend der Anforderungen an das System - ausgeführt werden sollten. Dieser Prozess umfasst folgende Aufgaben:

- Analysieren von Überwachungsdaten durch:
  - das Analysieren von Prozessen (Programme und Threads)
  - Informationen, ob die übermäßige Verwendung Hardwareressource die Systemleistung verringert
  - Informationen, ob es Auswirkungen von Engpässen oder aus sonstigen Gründen nicht hinreichend ausgelastete Hardwareressourcen gibt (z.B. Arbeitsspeicher, Festplattenspeicher...)
- Identifizieren von Bereichen mit inakzeptabler Leistung. Bei dieser Analyse kann möglicherweise festgestellt werden, dass die Systemleistung nicht jederzeit, abhängig von der Benutzerumgebung, ausreicht.
- Ausführen von korrigierenden Aktionen. Abhängig von den Gründen und dem Ausmaß der festgelegten Abweichungen, können korrigierende Aktionen durchgeführt werden.

# Untersuchen der Arbeitsspeicherleistung

Schlechte Arbeitsspeicherbedingungen können die Ausführung von Anwendungen und Diensten auf dem Computer verlangsamen und sich auf die Leistung anderer Systemressourcen auswirken.

Zum Einrichten einer Basislinie (Werte, in dem die Verwendung des physischen Arbeitsspeichers liegen kann) für die Verwendung des physischen Arbeitsspeichers, wird dieser bei Normalauslastung untersucht.

Die gesamte auf einem System ausgeführte Verarbeitung findet im Arbeitsspeicher statt, dabei muss sichergestellt werden, dass von diesem genügend zur Verfügung steht.

Folgende Leistungsindikatoren sind zum Untersuchen des **Speicher**-Objekts nützlich:

- Seiten/s zeigt die Anzahl von angeforderten Seiten an, die nicht sofort im RAM verfügbar waren
- Verfügbare Bytes zeigt an, wie viel physischer Arbeitsspeicher noch übrig ist

## Untersuchen von Auslagerungsdateien

Ein Mangel an Arbeitsspeicher wird durch ein häufiges Auslagern von Daten auf die Festplatte festgestellt. Die Auslagerung ist der Prozess, bei dem virtueller Arbeitsspeicher zwischen dem physischen Arbeitsspeicher und den Datenträger hinund herverschoben wird. Das Überprüfen der Auslagerungsdateigröße (empfohlen: verfügbares RAM \* 1,5) ist wichtig, um festzustellen ob sich eine Auslagerungsdatei im oberen Bereich des Grenzwertes befindet.

Folgende Leistungsindikatoren werden zum Überwachen der Größe von **Pagefile.sys** (Auslagerungsdatei) des **Auslagerungsdatei**-Objekts verwendet:

• Auslagerungsdatei\Belegung (%) dieser Wert liegt nah bei der Einstellung für die maximale Auslagerungsdatei\Generation 6 dateigröße

• Auslagerungsdatei\Max.Belegung (%) dieser Wert liegt nah bei 100%

## Untersuchen der Prozessorleistung

Prozessor **Prozessorzeit(%)** 

Zum Untersuchen der Prozessorleistung muss die Rolle des Computers und die Art der ausgeführten Arbeit berücksichtigt werden. Es gibt folgende nützliche Leistungsindikatoren:

•	1 10203301	1 102033012011(70)	zeigt den i lozentsatz der vergange
			nen Zeit an, während dessen ein
			Prozessor einen Tread ausführt. (Ein
			Wert von über 80% kann auf einen
			Engpass hinweisen)
•	System	Prozessor-	zeigt die Anzahl von derzeit in der
		Warteschlangenlänge	Prozessorwarteschlange befindlichen
			Thread an. (Eine Warteschlange mit
			zwei oder mehr Elementen kann bei
			einem Einprozessorsystem auf einen
			Engpass hinweisen)

zeigt den Prozentsatz der vergange-

Hohe Verwendungswerte können bei Arbeitsstationen auf eine effiziente Bearbeitung hinweisen. Beim Start eines neuen Prozesses kann die Prozessorzeit möglicherweise bis zu 100% ausgelastet sein (bei kurzeitiger Auslastung normal, bei langzeitiger Auslastung kritisch!).

Eine Prozessorauslastung von 100% auf einem Server, auf dem viele Clientanforderungen ausgeführt werden, weist auf einen Engpass hin und ist völlig inakzeptabel.

# Untersuchen der Datenträgerleistung

Das **Physikalischer Datenträger**-Objekt stellt Leistungsindikatoren für die Aktivität physischer Datenträger bereit, wohingegen das **Logischer Datenträger**-Objekt für Statistiken zu logischen Datenträgern und Speicherdatenträgern verantwortlich ist. Folgende Leistungsindikatoren sind zum Untersuchen der Datenträgerleistung nützlich:

•	Freier Speicherplatz	zeigt	den	Proz	zentsatz	an nich	t reserviertem
						_	

Speicherplatz in Bezug auf den gesamten verwendbaren Speicherplatz auf dem logi-

schen Datenträger an

• Mittlere Bytes/Übertragung ermittelt die Größe der Datenmengen bei

E/A-Operationen

• Mittlere Sek./Übertragung zeigt an, wie schnell Daten verschoben wer-

den (ein hoher Wert kann bedeuten, dass das System Anforderungen wegen langer Warteschlangen, oder aufgrund von Daten-

trägerfehlern wiederholt lesen muss)

Bytes/s zeigt die Übertragungsrate für Bytes an und

ist das primäre Maß für den Datenträger-

durchsatz

• Übertragungen/s zeigt die Anzahl von pro Sekunde ausge-

führten Lese- und Schreibvorgängen an (übersteigt der Wert 50 [beim Stripeset 50 pro physischem Datenträger], entsteht mög-

licherweise ein Engpass)

# Untersuchen der Netzwerkleistung

Der Systemmonitor (Leistungsaspekt) ermöglicht es, die Leistung der Netzwerkobjekte auf einem Server zu überwachen.

Folgende Leistungsindikatoren sind zum Untersuchen der Netzwerkaktivität nützlich:

#### • Netzwerkschnittstelle

<ul><li>Ausgabewarteschlangen</li></ul>	länge
---	-------

Ausgehende Pakete, verworfen

Gesamtzahl Bytes/s

Transmission Control Protocol (TCP)

Segmente empfangen/s

Erneut übertragene Segmente/s

Segmente/s

Segmente gesendet/s

zeigt die Ausgabewarteschlange für Pakete an hiermit kann bestimmt werden, ob das Netzwerk ,gesättigt' ist zum Überwachen der Netzwerkkartenleistung

Überwachen die Aktivität der Transportschicht

# • Internet Protocol (IP)

- Weitergeleitete Datagramme/s
- Datagramme empfangen/s
- Datagramme/s
- Datagramme gesendet/s

Überwachen die Aktivität der Netzwerkschicht

Der Netzwerkmonitor (Detailaspekt) kann zum Überwachen des Datenstromes im Netzwerk verwendet werden.

# **Unterrichtseinheit 9**

Sicherheitsrichtlinien werden verwendet, um die Sicherheit im Netzwerk zu verstärken. Die effizienteste Möglichkeit zum Implementieren dieser, stellt die Verwendung von *Sicherheitsvorlagen* (eine Textdatei, welche Sicherheitseinstellungen enthält, die zum Konfigurieren von Computern mit konsistenten Einstellungen verwendet werden) dar.

Es gibt zwei verschiedene Methoden, um Sicherheitsrichtlinien zu implementieren:

1. Mit Hilfe einer lokalen Systemrichtlinie auf einem einzelnen Computer (Start→Programme→Verwaltung→Lokale Sicherheitsrichtlinie)

Achtung: Diese Richtlinie wirkt sich nur auf den **lokalen** Computer aus!

 Über eine Gruppenrichtlinie in einer Domäne (Gruppenrichtlinien – welche in einen Gruppenrichtlinienobjekt [Group Policy Object, GPO] enthalten und einem Objekt in Active Directory zugeordnet sind definieren die von einem Systemadministrator verwalteten Komponenten der Desktopumgebung des Benutzers.

Achtung: Diese Richtlinie wirkt sich auf mehrere Computer in der Domäne aus!

# Implementieren einer lokalen Sicherheitsrichtlinie:

Start → Programme → Verwaltung → Lokale Sicherheitsrichtlinie → Kontorichtlinien

In der lokalen Sicherheitsrichtlinie die Konsole erweitern und auf die zu ändernde Option doppelklicken. In der rechten Hälfte der Konsole können nun die gewünschten Einstellungen getätigt werden. Diese sind eindeutig erklärt und können aktiviert oder deaktiviert werden.

# Implementieren von Sicherheit auf mehreren Computern

Erstellt werden Gruppenrichtlinien mit Hilfe der Microsoft Management Console kurz MMC. (Start -> Programme -> MMC)

Detaillierte Anleitung in den MOC Unterlagen Kapitel 9 Übung 1,2,3 oder in der Windows Hilfe unter MMC.

Wichtig: Gruppenrichtlinieneinstellungen werden in der folgenden Reihenfolge übernommen: Zuerst werden lokale Einstellungen, dann Standort- und Domäneneinstellungen und schließlich Organisationseinheiteneinstellungen übernommen.

# Ändern der Sicherheitseinstellungen

Folgende Liste beschreibt die Sicherheitseinstellungen, die unter Verwendung der **lokalen Sicherheitsrichtlinie**, oder der Erweiterung für Sicherheitseinstellungen in der **Gruppenrichtlinie** für Computer konfiguriert werden können:

Kontorichtlinien
 Konfigurieren des Kennwortes und der Konto-

richtlinien (primäres Sicherheitsprotokoll inner-

halb einer Domäne → Kerberos V5)

Lokale Richtlinien Konfigurieren der lokalen Überwachung, Be-

nutzerrechte und Sicherheitsoptionen

• Richtlinien öffentlicher Schlüssel Konfigurieren von Agenten für die Wie-

derherstellung von verschlüsselten Daten, Domänenstämmen, vertrauenswürdigen Zertifizierungsstellen, etc.

■ *IP-Sicherheitsrichtlinien* Konfigurieren der IP Sicherheit (Internet Protocol

Security, IPSec) in einem Netzwerk und der Kommunikation in einem Intranet, bzw. virtuellen privaten Netzwerk (VPN) über das

Internet.

Die folgenden Sicherheitsrichtlinien können nur mit Hilfe der Erweiterung für Sicherheitseinstellungen in der Gruppenrichtlinie konfiguriert werden:

• Ereignisprotokoll Konfigurieren der Einstellungen für Anwen-

dungs-, System- und Sicherheitsprotokolle

Eingeschränkte Gruppen Konfigurieren von Gruppenmitgliedschaften für

vordefinierte/sicherheitsgefährdete Gruppen (Administratoren , Domänenadmins usw.) mit

bestimmten vordefinierten Funktionen

Systemdienste Konfigurieren der Sicherheits- und Starteinstel-

lungen für Dienste, die auf einem Computer

ausgeführt werden

Registrierung
 Konfigurieren der Sicherheit für Registrierungs-

schlüssel

Dateisystem Konfigurieren der Sicherheit für bestimmte

Dateipfade

## Verwenden von vordefinierten Sicherheitsvorlagen

Vordefinierte Vorlagen können häufig einen Startpunkt zum Anpassen einer idealen Sicherheitskonfiguration bereitstellen. Die unter Windows 2000 vordefinierten Sicherheitsvorlagen (ändern die Standardsicherheitseinstellungen inkrementell) wurden entworfen, um allgemeine Sicherheitsanforderungen zu erfüllen. Sie schließen Vorlagen ein, die vier Sicherheitsstufen bieten :

- Basis (definieren die Standardsicherheitsstufe für W2K)
- Kompatibel (höhere Sicherheitsstufe als Basis)
- **Sicher** (zusätzliche Sicherheitsstufe gegenüber Kompatibel)
- Sehr Sicher (höchste Sicherheitsstufe für W2K)

*Wichtig:* Beim Aktualisieren von Computern unter Microsoft WinNT 4.0, welche mit dem NTFS-System laufen, wird die Sicherheit <u>nicht</u> geändert. Sie bleibt jedoch unter der Windows 2000 Sicherheitsstufe Basis.

Falls beim Aktualisieren von WinNT 4.0 auf Windows 2000 die Partition in eine FAT Partition umgewandelt wird, kann die Sicherheit für diesen Computer nicht übernommen werden.

Sicherheitsstufe	Workstation Server		Domänencontroller
Basis	Basicwk.inf Basicsv.inf		Basicdc.inf
Kompatibel	Kompatibel Compatws.inf		nicht in diesem Modus
Sicher	Securews.inf		Securedc.inf
Sehr Sicher	Hisecw	s.inf	Hisecdc.inf

Es wird nicht gewährleistet, das in den Stufen **Sicher** und **Sehr Sicher** (sicherer Server) alle Features der Standardanwendungen ausgeführt werden können. Die Basis-Vorlagen befinden sich im Ordner **%SystemRoot%\Security\Templates** 

# Erstellen von benutzerdefinierten Sicherheitsvorlagen

- 1. Microsoft Management Console (MMC) starten
- 2. Snap-In hinzufügen
- 3. Auswählen der anzupassenden Vorlage (%SystemRoot%\Security\Templates)
- 4. Konfigurieren der neuen Richtlinieneinstellungen
- 5. Speichern der neuen Konfiguration

Im Gegensatz zur Verwendung der Grafischen Oberfläche ist es ebenso möglich, die Eingabeaufforderung zum Ausführen der Sicherheitskonfiguration und –analyse mit Hilfe von Skriptdateien zu verwenden. Das Programm, das hierzu verwendet wird ist **SECEDIT.EXE**. Es stellt einige Funktionen bereit (wie beispielsweise das

Aktualisieren einer Sicherheitsrichtlinie), welche auf der grafischen Benutzeroberfläche nicht verfügbar sind.

Folgende Schalter, bzw. Optionen werden bei SECEDIT.EXE auf höherer Ebene ausgeführt:

- /analyze
- /configure
- /export
- /refreshpolicy (ermöglicht das Erzwingen eines Gruppenrichtlinienüber-

mittlungsereignisses)

- /validate (überprüft die Syntax einer Vorlage)
- /areas (bestimmte Bereiche der Sicherheitseinstellungen können

konfiguriert und exportiert werden)

# Überwachung des Zugriffs auf Systemressourcen

# Einführung in die Überwachung

Die Überwachung (nur im NTFS-Systemen möglich) stellt den Vorgang des Nachverfolgens von Benutzer- und Betriebssystemaktivitäten (Ereignisse) auf einem Computer dar. (Eintrag zu dem Ereignis im Sicherheitsprotokoll)

## Überwachungseinträge

Ein Überwachungseintrag im Sicherheitsprotokoll enthält folgende Informationen:

- Den ausgeführten Vorgang
- Den Benutzer, der den Vorgang ausgeführt hat
- Erfolg oder Fehlschlag und den Zeitpunkt des Ereignisses
- Weitere Informationen, wie z.B. der Computer auf dem das Ausführen des Vorgangs ausgeführt/versucht wurde

# Überwachungsrichtlinie

Eine Überwachungsrichtlinie definiert die Typen von Sicherheitsereignissen, die Windows 2000 im Sicherheitsprotokoll auf jedem Computer protokolliert. Windows 2000 schreibt die Ereignisse in das Sicherheitsprotokoll auf dem entsprechenden Computer, auf dem das jeweilige Ereignis aufgetreten ist.

### Anzeigen von Ereignissen

Die Konsole **Ereignisanzeige** wird verwendet, um die von Windows 2000 im Sicherheitsprotokoll aufgezeichneten Ereignisse anzeigen zu lassen. Protokolldateien können auch archiviert werden, um Trends über einen längeren Zeitraum nachzuverfolgen. Protokolldateien werden mit der Dateiendung **.evt** (Eventlog) abgespeichert.

# Folgende Ereignisse können überwacht werden :

Anmeldeversuche z.B. das Anmelden eines Benutzers wird in der

Kategorie Kontoanmeldung protokolliert

• Kontenverwaltung erstellen, umbenennen, aktivieren oder deaktivieren

eines Kontos; Kennwort festlegen oder ändern

Active Directory Zugriffe Ein Benutzer erhält Zugriff auf ein Active Directory

Objekt

Anmeldeereignisse
 An- und Abmelden eines Benutzers, Herstellen

einer Netzwerkverbindung; wird auf dem Computer, auf den der Benutzer zugreift, protokolliert (unabhängig davon, ob dieser ein lokales- oder ein Do-

mänenkonto verwendet)

Objektzugriffsversuche Benutzer erhält Zugriff auf eine Datei, Ordner usw.

Richtlinienänderung Änderung an den Sicherheitsoptionen, Benutzer-

rechten oder Überwachungsrichtlinien

Rechteverwendung
Benutzer nimmt ein Recht war: z.B. ändern der

Systemzeit, oder Administrator übernimmt die Be-

sitzrechte für eine Datei

Prozessverfolgung
 Eine Anwendung führt einen Vorgang aus

Systemereignisse
 Neustart oder Herunterfahren des Rechners, oder

es ist ein Ereignis aufgetreten, das sich auf die Sicherheit von Windows 2000 oder auf das Sicher-

heitsprotokoll auswirkt

# Planen einer Überwachungsrichtlinie

Werden zu viele Ereignistypen überwacht, so kann dies zu einer erheblichen Überlastung und somit auch zu einer Verringerung der Systemleistung führen. Daher sollten nur wirklich nützliche Informationen für die Sicherheitsmaßnahmen überwacht werden.

Zum Planen einer Überwachungsrichtlinie sollte folgendes beachtet werden:

- Bestimmung der zu überwachenden Computer
- Bestimmung der zu überwachenden Ereignisse
- Bestimmung, ob Erfolg oder Fehlschlag (oder beides) überwacht werden soll
- Bestimmung, ob Trends nachverfolgt werden müssen
- Regelmäßige Überprüfung der Sicherheitsprotokolle

# Einrichten einer Überwachungsrichtlinie

- 1) Erstellung einer MMC-Konsole und einfügen des Snap-In`s **Gruppenrichtlinie**. **Lokaler Computer** wird als Gruppenrichtlinienobjekt ausgewählt.
- 2) Erweitern der Option Computerkonfiguration unter Richtlinien für lokaler Computer → Windows-Einstellungen → Sicherheitseinstellungen → Lokale Richtlinien → Überwachungsrichtlinien

**Achtung:** Um eine Überwachungsrichtlinie konfigurieren zu können, muss man Mitglied der Gruppe Administratoren sein!

# Unterrichtseinheit 10

# Begriffe zum Drucken unter Windows 2000

### Druckgerät

Das Hardwaregerät, an dem die gedruckten Dokumente entnommen werden können.

Windows 2000 unterstützt folgende Druckgeräte:

- Lokale Druckgeräte: Druckgeräte, die mit einem physischen Anschluss (z.B. LPT1) des Druckservers verbunden sind
- Netzwerkdruckgeräte: Druckgeräte, die über das Netzwerk (eigener oder externer Netzwerkadapter mit eigener IP-Adresse) und nicht über einen physischen Anschluss mit dem Druckserver verbunden sind.

#### Drucker

Die Softwareschnittstelle zwischen dem Betriebssystem und dem Druckgerät. Sie definiert wann und wohin ein Dokument gesendet wird, um ein Druckgerät über einen physischen Anschluss oder im Netzwerk zu erreichen. Ebenso gilt dies für das Drucken in eine Datei (Endung .prn).

#### Druckserver

Der Computer, auf dem sich die Drucker- und Clienttreiber befinden. Er empfängt Dokumente von Clients und verarbeitet sie. Auf dem Druckserver werden **Drucker**, die mit **lokalen oder Netzwerkdruckgeräten** verbunden sind eingerichtet und freigegeben.

#### Druckertreiber

Auf dem Druckserver muss der geeignete Druckertreiber (Dateien mit Informationen für Druckerbefehle) für die jeweiligen Clients verfügbar sein.

# Anforderungen für das Konfigurieren eines Netzwerkdruckers

- Ein Druckserver auf dem folgendes ausgeführt wird:
  - Ein Betriebssystem der Windows 2000 **Serverfamilie**, wenn eine große Anzahl von Verbindungen erforderlich ist

#### oder

- Windows2000 **Professional** für Netzwerke mit 10 oder weniger gleichzeitig verbundenen Clientcomputern
- Genügend Arbeitsspeicher, um Dokumente verarbeiten zu können
- Ausreichend Speicherplatz auf der Festplatte des Druckservers, um Dokumente zu speichern, bis sie gedruckt werden.

Um einen Drucker hinzuzufügen und im Netzwerk freizugeben, muss man sich als Administrator am Druckserver anmelden. Anschließend verwendet man den Druckerinstallations-Assistenten (*Start* → *Einstellungen* → *Drucker* → *neuer Drucker*), um einen Drucker hinzuzufügen und freizugeben.

Achtung: Wird ein anderes Netzwerkprotokoll als TCP/IP verwendet, muß dieses erst installiert werden, bevor der Drucker-Installationsassistent gestartet wird!

# Hinzufügen und Freigeben eines Druckers für ein lokales Druckgerät

Die Anzahl der lokalen Druckgeräte, die mittels physischer Anschlüsse mit einem Druckserver verbinden werden können, hängt von der jeweiligen Hardwarekonfiguration ab.

Folgende Optionen werden vom Drucker-Installationsassistenten zum Hinzufügen eines Drucker für ein lokales Druckgerät bereitgestellt:

- Lokaler Drucker
- Vorhandenen Anschluss verwenden

<u>Möglichkeit 1:</u> **vorhandenen Anschluss verwenden**Der Anschluss am Druckserver, an dem das Druckgerät angeschlossen ist (physischer Standardanschluss z.B. LPT1)

Möglichkeit 2: einen neuen Anschluss erstellen Hiermit kann ein neuer Anschluss hinzugefügt werden, der nicht als Standard-Anschluss gilt (z.B. eine Netzwerkverbindung)

- Hersteller und Drucker
- Druckername
- Standarddrucker
- Freigegeben als
- Standort und Kommentar
- Soll eine Testseite gedruckt werden?

# Hinzufügen und Freigeben eines Druckers für ein Netzwerkdruckgerät

In größeren Organisationen handelt es sich bei den meisten Druckgeräten um Netzwerkdruckgeräte.

#### Vorteile:

- ➤ Höhere Flexibilität hinsichtlich des Druckgerätestandortes
- Schnellere Datenübertragung, da Netzwerkverbindungen und nicht Druckerverbindungskabel verwendet werden

Um einen Drucker für ein Netzwerkdruckgerät hinzuzufügen und freizugeben, kann der Drucker-Installationsassistent verwendet werden. Das Protokoll, das von vielen Druckgeräten verwendet wird ist TCP/IP. Unter Windows 2000 ist dieses Protokoll standardmäßig installiert. Die Verwendung von TCP/IP erfordert zusätzliche Anschlussinformationen zum Hinzufügen eines Standard-TCP/IP-Druckerports.

Folgende Optionen werden vom Drucker-Installationsassistenten zum Hinzufügen eines Drucker für ein Netzwerkdruckgerät bereitgestellt:

- einen neuen Anschluss erstellen
- Typ

**Anmerkung:** Wird ein Netzwerkdrucker hinzugefügt und freigegeben, so ist er automatisch im Active Directory veröffentlicht. Es ist dadurch einfacher einen Drucker im Netzwerk zu suchen.

# <u>Verwenden des Assistenten zum Hinzufügen eines Standard-TCP/IP-Druckerports</u>

Dieser wird gestartet, wenn unter "einen neuen Anschluss hinzufügen" der Standard TCP/IP – Port ausgewählt wird.

#### Benötigte Informationen:

- Druckernamen oder IP-Adresse
- Portname

## Einrichten von Clientcomputern

Nachdem ein Drucker hinzugefügt und freigegeben wurde, muss auf alle Clientcomputer, die auf diesen Druckserver zugreifen, der geeignete Druckertreiber installiert werden.

- Clientcomputer unter folgenden Betriebssystemen führen nach erfolgreicher Verbindung einen automatischen Download des geeigneten Druckertreibers vom Druckserver durch:
  - ✓ Windows 95 , Windows 98
  - ✓ Windows NT
  - ✓ Geeignete Druckertreiber müssen auf dem Druckserver vorhanden sein. Eine Aktualisierung der Treiberdateien ist somit auch nur auf dem Druckserver notwendig, da Clients die aktualisierten Treiber automatisch beim nächsten Druckauftrag downloaden
- Clientcomputer unter anderen Microsoft-Betriebssystemen (z.B. Win3.xx, MS-DOS) erfordern die manuelle lokale Installation des Treibers
- Clientcomputer unter Nicht-Microsoft-Betriebssystemen erfordern die Installation von:
  - ✓ dem Druckertreiber auf dem Clientcomputer
  - ✓ einen Druckdienst, die verwendeten Protokolle, sowie deren geeigneten Zusatzdienste (für die Clients) auf dem Druckserver

- Macintosh → Dienste für Macintosh sind in Windows 2000-Server enthalten, werden aber nicht standardmäßig installiert
- Unix → TCP/IP Druckserver (Line Printer Dämon, LPD) ist in Windows 2000-Server enthalten, wird aber nicht standardmäßig installiert
- Netware → File und Print Services für Netware ist ein optionaler Add-On-Dienst für Windows 2000-Server und ist nicht in Windows2000 Server enthalten

## Konfigurieren eines Netzwerkdruckers

### 1. Freigeben eines vorhandenen Druckers

Um einen Drucker auf einem Druckserver freizugeben sind folgende Schritte erforderlich oder möglich:

- dem Drucker einen intuitiven Freigabenamen zuweisen, der unter der Netzwerkumgebung angezeigt wird
- der Drucker kann im Active Directory veröffentlicht werden (im Active Directory können Benutzer den Drucker schneller finden)
- zusätzliche Druckertreiber für unterschiedliche Hardwareplattformen auf dem Druckserver installieren (siehe Einrichten von Clientcomputern)

Zugriff auf die Registerkarte **Freigabe** erhält man im Ordner Drucker, indem man mit der rechten Maustaste auf das Symbol für den Drucker klickt, den man freigeben möchte.

#### 2. Einrichten eines Druckerpools

#### **Definition:**

Ein Druckerpool besteht aus einem **Drucker**, der über **mehrere Anschlüsse** an einem **Druckserver mit mehreren Druckgeräten** (lokal oder Netzwerk) verbunden ist. Die Druckgeräte müssen <u>nicht</u> identisch sein, sie müssen jedoch <u>denselben</u> **Druckertreiber** verwenden.

Wenn ein Druckerpool erstellt wird, können Benutzer Dokumente drucken, ohne zuvor das verfügbare Druckgerät bestimmen zu müssen. Die Ermittlung eines verfügbaren Anschlusses wird stattdessen vom **Drucker** vorgenommen.

Die Verwendung eines Druckerpools bietet die folgenden Vorzüge:

- Die Zeit, für die ein Dokument auf dem Druckserver gespeichert werden muss, verkürzt sich
- Vereinfachte Verwaltung, da ein Druckerpool mehrere Druckgeräte über einen einzigen Drucker verwalten kann

#### Erstellung eines Druckerpools:

- 1. Dialogfeld **Eigenschaften** des Druckers öffnen
- 2. Unter der Registerkarte Anschlüsse das Kontrollkästchen **Druckerpool aktivieren** aktivieren
- 3. Jeden Anschluss, an dem ein Druckgerät angeschlossen wird, aktivieren

## 3. Festlegen von Druckerprioritäten

Durch das Festlegen von Druckerprioritäten (1 niedrig - 99 hoch) für Druckaufträge, die auf demselben Druckgerät gedruckt werden, müssen mehrere Drucker, die auf dasselbe Druckgerät verweisen, erstellt werden.

Um Prioritäten zwischen Druckern festzulegen, müssen folgende Schritte ausgeführt werden:

- 1. Konfigurieren zweier oder mehrerer Drucker, so dass diese auf dasselbe Druckgerät (denselben Anschluss → physisch oder Netz)
- 2. Für jeden Drucker eine andere Priorität festlegen; anschließend kann jede Benutzergruppe angewiesen werden, ihre Dokumente an einen anderen Drucker (mit dementsprechender Priorität) zu senden.

Um die Priorität eines Druckers festzulegen sind folgende Schritte durchzuführen:

- 1. Dialogfeld **Eigenschaften** des Druckers öffnen
- 2. Auf der Registerkarte Erweitert im Drehfeld Priorität die gewünschte Priorität festlegen

#### 4. Zuweisen von Druckerberechtigungen

Es stehen drei Ebenen für die Druckerberechtigungen zur Verfügung: Drucken (niedrigste), Dokumente verwalten (mittlere) und Drucker verwalten (höchste)

Die Administratoren eines Servers, sowie die Druck- und Serveroperatoren eines Domänencontrollers verfügen standardmäßig über die Berechtigung **Drucker verwalten**, die Gruppe **Jeder** über **Drucken** und der Besitzer eines Dokuments über **Dokumente verwalten**.

Um einen Benutzer oder eine Gruppe Druckerberechtigungen zuzuweisen, sind folgende Schritte durchzuführen:

- 1. Mit der rechten Maustaste im Ordner Drucker auf das Symbol des Druckers, für den die Berechtigungen geändert werden sollen und anschließend auf **Eigenschaften** klicken
- 2. Auf der Registerkarte **Sicherheitseinstellungen** die Gruppe **Jeder** entfernen und anschließend auf der Schaltfläche **Hinzufügen** die entsprechenden Benutzer und Gruppen auswählen und die Berechtigungen hinzufügen

In der folgenden Tabelle sind die Operationen aufgeführt, zu deren Durchführung die unterschiedlichen Ebenen berechtigen.

	_		
Zugelassene Aktionen	Drucken	Dokumente verwalten	Drucker verwalten
Drucken von Dokumenten	х	Х	х
Anhalten, Fortsetzen, erneutes Starten und Abbrechen des Druckvorgangs für das eigene Dokument	х	х	х
Herstellen einer Verbindung zum Drucker	х	X	x
Steuern der Auftragseinstel- lungen für alle Dokumente		Х	Х
Anhalten, erneutes starten und Löschen des Druckvorgangs für alle Dokumente		X	x
Freigeben eines Druckers			Х
Ändern von Druckereigen- schaften			x
Löschen von Druckern			Х
Ändern von Druckerberechti- gungen			Х

# Konfigurieren des Internetdruckens

Dies ist ein neues Feature in Windows 2000. Damit besteht die Möglichkeit, mit Hilfe eines Webbrowsers Druckaufträge an Drucker im Internet (IPP, Internet Printing Protocol) oder einem Intranet zu senden und Drucker mit diesen zu verwalten. Weiterhin können Drucker direkt an eine URL drucken und die Informationen zu Druckaufträgen im HTML-Format anzeigen.

# Einrichten des Internetdruckens mit Hilfe eines Webbrowsers

### Die Anforderungen für das Drucken mit Hilfe eines Webbrowsers sind

- Der Drucker muss freigegeben sein
- Druckserver muss unter Windows 2000 Server mit Microsoft IIS (Internet Informations Service) oder Windows 2000 Professional auf dem der Peer Web-Server (PWS) ausgeführt werden
- Internet Explorer 4.0 oder höher muss auf dem Clientcomputer installiert sein (Netscape geht nicht)

## Um mit Hilfe eines Webbrowsers eine Verbindung zu einem Drucker herzustellen, ist folgendes erforderlich:

- URL des Druckers muss bekannt sein
- Erforderliche Berechtigungen zum Herstellen einer Verbindung zum Drucker müssen vorliegen

#### Adresse im Webbrowser für den Drucker:

http://<Name des Druckerservers>/printers

### Um eine Verbindung zu einem Internetdrucker herzustellen kann der Druckerinstallations-Assistenten verwendet werden.

Bei einem sehr hohen Druckaufkommen kann es von Vorteil sein, nicht den Standardspoolordner zu verwenden, sondern das Spoolverzeichnis des Druckservers in einen Ordner einer anderen Partition umzuleiten.

Um ein Spoolverzeichnis (Spoolordner) umzuleiten, schlägt Microsoft folgenden Weg vor:

- 1. Start→Einstellungen→Drucker
- 2. Datei→Servereigenschaften
- 3. Eigenschaften von Druckserver→Erweiterte Optionen→Spoolordner
- 4. gewünschten Ordner eingeben und **OK** klicken
- 5. im Meldungsfeld **Eigenschaften von Druckserver** auf **Ja** anklicken

# Unterrichtseinheit 11

# Konfigurieren der Hardware für mobile Datenverarbeitung

Unter Windows 2000 ist es möglich mehrere Profile für verschiedene Umgebungen, einschließlich Dockingstationen zu konfigurieren. Jedoch ist für tragbare Computer, die sowohl in einer Dockingstation als auch als eigenständige Computer verwendet werden, unter Umständen eine erweiterte Konfiguration erforderlich.

# Erstellen eines Hardwareprofils für mobile Benutzer

Windows 2000 erkennt bei neueren Laptops automatisch die Hardware. Geschieht dies aus irgendeinem Grund nicht (z.B. veraltetes BIOS), so kann ein Hardwareprofil erstellt werden, in dem die Profile für die Geräte bestimmt werden, die ein portabler Computer lädt, wenn ein Benutzer den Computer aus einer Dockingstation im Netzwerk entnimmt und als eigenständigen Computer an einem Remotestandort verwendet.

#### Hardwareprofile werden erstellt unter:

Start → Einstellungen → Systemsteuerung → System → Hardware → Hardwareprofile

Um ein spezifisches Profil zu erstellen, muss zuerst eine Kopie des vorhandenen Profils (aktuell) erstellt werden. Diese Kopie sollte dann so umbenannt werden, dass die Funktion des Profils eindeutig an ihrem Namen erkennbar ist. Danach wird eine Startoption unter Beim Start von Windows ausgewählt und ein Neustart des Computers durchgeführt, um den Rechner mit dem gerade kopierten Profil zu starten. Nach erfolgreichem Start kann das gewählte Profil nun den gewünschten Anforderungen angepasst werden. Um bestimmte Geräte beim Start zu laden bzw. nicht zu laden, muss im **Gerätemanager** (Start → Einstellungen → Systemsteuerung → System → Hardware → Gerätemanager) das jeweilige Gerät ausgewählt und unter **Geräteverwendung** aktiviert oder deaktiviert werden.

# Verwenden von Dockingstationen

Windows 2000 Professional verfügt über eine integrierte Unterstützung für Dockingstationen. Benutzer können tragbare Computer an einer Dockingstation anschließen, bzw. daraus entfernen, ohne einen Neustart durchzuführen. Diesen Vorgang bezeichnet man als warm docking.

Um einen tragbaren Computer aus der Dockingstation zu entfernen, schlägt Microsoft folgenden Weg vor:

#### Start → PC trennen

## Konfigurieren der Energieverwaltungsoptionen für mobile Datenverarbeitung

Windows 2000 Professional unterstützt eine Energieverwaltungstechnologie mit dem Namen ACPI (Advanced Configuration and Power Interface). Es schließt ausserdem die Unterstützung für tragbare Computer ein, die APM (Advanced Power Management) verwenden.

Ein Energieschema wird folgendermaßen ausgewählt:

 $Start \rightarrow Einstellungen \rightarrow Systemsteuerung \rightarrow Energieoptionen \rightarrow Energieschemas$ 

Auf der Registerkarte Energieschemas kann unter folgenden Energieschemas gewählt werden:

- Desktop
- Tragbar/Laptop
- Präsentation
- Dauerbetrieb
- Minimaler Energieverbrauch
- Minimale Batteriebelastung

### Verwenden von Energiesparoptionen

Es gibt im wesentlichen zwei Energiesparoptionen unter Windows 2000 Professional

#### Standby

- Für eine <u>kurze</u> Zeit der Abwesenheit
- Monitor und Festplatten werden automatisch abgeschaltet
- Das Betriebssystem wird weiterhin in einem Zustand mit niedriger Energiezufuhr ausgeführt

#### Ruhezustand

- Für eine längere Zeit der Abwesenheit
- Der Desktop wird auf die Festplatte gespeichert
- Monitor und Festplatten werden automatisch abgeschaltet
- Das System wird heruntergefahren

Vorraussetzung: Der Computer muss diese Energiesparfunktionen unterstützen!!!

#### Wichtig:

Da im Standbymodus der Desktopstatus <u>nicht</u> auf die Festplatte gespeichert wird, kann ein Stromausfall während dieses Modus bewirken, dass nicht gespeicherte Daten verloren gehen.

Der Ruhezustand, in dem der Computer runtergefahren wird, erfordert den freien Speicherplatz auf der Bootpartition, der dem internen RAM des Computers entspricht.

Das Windows Kennwort kann sowohl für den Standbymodus, als auch für den Ruhezustand verwendet werden. Um seinen Computer während des Standbymodus oder Ruhezustands durch ein Kennwort zu sichern, muss unter den Energieoptionen auf die Registerkarte Erweitert geklickt und Kennwort beim Reaktivieren des Computers anfordern ausgewählt werden.

### Verfügbarmachen von Dateien für Offlineverwendung

#### Einführung in Offlinedateien

- Der Benutzer meldet sich ab
  - Lokale Dateien werden mit Dateien auf dem Server synchronisiert
- Der Benutzer ist vom Netzwerk getrennt
  - Der Benutzer arbeitet mit der lokalen Kopie der Datei
- Der Benutzer meldet sich an
  - Lokale Dateien werden mit den Dateien auf dem Server synchronisiert

### Konfigurieren eines Servers für Offlinedateien

Standardmäßig ist für jeden freigegebenen Ordner auf einem Computer unter Windows 2000 oder Advanced Server die Verwendung von Offlinedateien aktiviert.

Um die Zwischenspeicherungsoptionen für einen freigegebenen Ordner festzulegen, sind folgende Schritte auszuführen :

- Im Explorer mit der Rechten Maustaste auf den entsprechenden Ordner, dann auf Eigenschaften, Freigabe und anschließend auf Zwischenspeichern klicken
- Wenn der Inhalt des Ordners <u>nicht</u> zwischengespeichert werden soll (deaktivieren von Offlinedateien für einen öffentlichen Ordner), das Kästchen Zwischenspeichern der Dateien in diesem freigegebenem Ordner zulassen deaktivieren.

Andernfalls ist die Zwischenspeicherung aktiviert (Offlinedateien verfügbar) und es können folgende Optionen ausgewählt werden:

- Manuelles Zwischenspeichern für Dokumente
  - Nur Dateien, die vom Benutzer **speziell markiert** wurden, werden zwischengespeichert (**Standardeinstellung**)
- Automatisches Zwischenspeichern für Dokumente
  - Dateien werden **automatisch beim ersten Öffnen** zwischengespeichert. Ältere Dateien werden dabei gelöscht.

#### Automatisches Zwischenspeichern für Programme

 ermöglicht das Zwischenspeichern in eine Richtung für schreibgeschützte Dateien und Anwendungen, welche einmal auf der lokalen Festplatte zwischengespeichert und nicht wieder zurück auf den Server zurückgeschrieben und repliziert werden. Es wird mit der lokalen Kopie auf dem Client weitergearbeitet. Original werden somit nicht abgeändert und überschrieben.

## Konfigurieren eines Clientcomputers für Offlinedateien

Um eine Datei, bzw. einen Ordner für die Offlineverwendung für einen Client verfügbar zu machen, muss folgendes ausgeführt werden:

- 1. Windows Explorer → Extras → Ordneroptionen
- 2. Auf der Registerkarte **Offlinedateien** das Kontrollkästchen **Offlinedateien aktivieren**.

Ist der Computer **offline**, so werden die (Offline-)Dateien im **selben Verzeichnis** durch einen **Doppelpfeil** angezeigt, in dem sie **online** angezeigt wurden.

# Verwenden der Synchronisationsverwaltung zum Synchronisieren von Dateien

Werden Offlinedateien eingerichtet, synchronisiert Windows 2000 diese standardmäßig automatisch, sobald ein Benutzer die Verbindung zum Netzwerk trennt oder erneut herstellt.

Um die Synchronisationsverwaltung zu öffnen und Synchronisationseinstellungen zu konfigurieren, müssen folgende Schritte durchgeführt werden:

- 1. Start → Programme → Zubehör → Synchronisieren
- 2. Unter **Zu synchronisierende Objekte** die Kontrollkästchen für die Offlineobjekte, die synchronisiert werden sollen, aktivieren
- 3. Auf Einrichten klicken, um das Dialogfeld Synchronisationseinstellungen anzuzeigen, danach entweder eine LAN- oder DFÜ-Verbindung auswählen

## Herstellen von Verbindungen zu Netzwerken und Computern

Um eine Verbindung zu einem Remotenetzwerk (private oder Internet Service Provider [ISP]) oder –computer herstellen zu können, muss mittels des Verbindungsassistenten eine neue DFÜ-Verbindung auf dem Clientcomputer erstellt werden.

# Start → Einstellungen → Netzwerk und DFÜ Verbindungen → Neue Verbindung erstellen

## <u>Herstellen von Verbindungen zu einem privaten Netzwerk über das</u> Internet

Der Netzwerkverbindungsassistent wird ebenfalls verwendet, um über das Internet eine Verbindung zu einem privaten Netzwerk (VPN – Virtual Private Network) herzustellen. Ein VPN verwendet Tunneling Protokolle wie das Point-to-Point-Tunneling-Protokoll (PPTP) oder das Layer-2-Tunneling Protokoll (L2TP) über ein ungesichertes Netzwerk, um Remoteclients den Zugriff auf ein Unternehmensnetzwerk bereitzustellen.

**Vorteil:** Verbindungskosten werden deutlich reduziert, da keine Gebühren für Ferngespräche, sondern nur die jeweiligen Minutenpreise des jeweiligen Internet Service Providers anfallen.

Der Verbindungsassistent wird folgendermaßen gestartet:

Start → Einstellungen → Netzwerk und DFÜ Verbindungen → Neue Verbindung erstellen → Verbindung mit einem privaten Netzwerk über das Internet herstellen

Der Netzwerk-Verbindungsassistent kann aber auch über ein Parallelkabel (Standard- und der erweiterte Parallelport [ECP]) oder Infrarotgerät (auf beiden Computern ein Infrarot-Transceiver mit einem maximalen Abstand von 1m) eine direkte Verbindung zu einem anderen Computer erstellen.

Start → Einstellungen → Netzwerk und DFÜ Verbindungen → Neue Verbindung erstellen → Direkt mit anderen Computer verbinden

# **Unterrichtseinheit 12**

### Festplattentypen von Windows 2000

Bei Windows 2000 wird beim Implementieren von Datenträgern zwischen zwei Arten von Festplattentypen unterschieden :

- Basisfestplatten
- Dynamische Festplatten

Der ausgewählte Festplattentyp bestimmt, wie der Speicherplatz auf der Festplatte verwendet wird. Dynamische Festplatten stellen mehr Flexibilität bereit als Basisfestplatten. Man kann auf einer dynamischen Platte **Fehlertoleranz** implementieren, was auf einer Basisplatte hingegen nicht möglich ist.

### Basisfestplatten

Eine Basisfestplatte ist das Standardspeichermedium für Windows 2000. Wird eine neue Festplatte installiert, so wird diese von Windows 2000 erkannt und **standard-mäßig als Basisfestplatte** konfiguriert.

#### Die Merkmale einer Basisfestplatte sind wie folgt :

- Sie kann bis zu vier Partitionen enthalten
- Sie ist mit anderen Typen von Datenträgerspeichern kompatibel (z.B. Stripsets und vorher vorhandenen Datenträgersätzen unter NT4.0 und anderen OS)

#### Die dabei möglichen Partitionstypen sind:

- Primäre Partition (bis zu vier möglich)
- Erweiterte Partition mit logischen Laufwerken

<u>Wichtig:</u> Auf einer Windows 2000 Basisfestplatte können keine <u>neuen</u> Datenträgersätze, Stripesets oder RAID-5-Sätze erstellt werden ( **keine Fehlertoleranz** ).

Laufwerksbuchstaben <u>und</u> Partitionsnummer werden <u>erst</u> an primäre und dann an erweiterte Partitionen verteilt.

Falls eine Konvertierung von einer Basisfestplatte in eine dynamische Festplatte vorgenommen wird, sollte beachtet werden, dass beim Erstellen der Partition mindestens **1 MB** nicht zugeordneter Speicherplatz übrig bleibt.

### Dynamische Festplatten

Vorteile von dynamischen Festplatten:

 Eine dynamische Festplatte kann nicht zusammenhängenden Speicherplatz auf jeder verfügbaren Festplatte einschließen

- Die Anzahl der Datenträger pro Festplatte ist nicht begrenzt (somit auch nicht abhängig von Laufwerksbuchstaben )
- Win2000 speichert die Informationen zur Festplattenkonfiguration nicht mehr in der Registrierung, sondern auf der Festplatte (deshalb 1MB frei lassen) ab. Die Informationen werden auf alle anderen dynamischen Festplatten repliziert, so dass der Ausfall einer einzelnen Platte sich nicht auf den Datenzugriff auf andere Festplatten auswirkt.
- Implementierung von Fehlertoleranz möglich

Eine Festplatte kann entweder eine Basisfestplatte oder eine dynamische Festplatte sein. Eine Kombination beider Speichertypen auf einer Festplatte ist nicht möglich. Verfügt der Computer jedoch über mehrere Festplatten, so kann jede Platte entweder als Basis- oder dynamische Festplatte konfiguriert werden.

### Erstellen von Partitionen auf einer Basisfestplatte

Alle Einstellungen, die Festplatten betreffen sind in der Datenträgerverwaltung zu konfigurieren.

### Start → Programme → Verwaltung → Computerverwaltung → Datenträgerverwaltung

## Erstellen von Datenträgern auf einer dynamischen Festplatte

Eine neu installierte Platte wird unter Win2000 standardmäßig als Basisfestplatte erstellt. Um eine dynamische Festplatte daraus zu machen, muss die Basisfestplatte auf eine dynamische Festplatte aktualisiert werden.

# Aktualisieren von einer Basisfestplatte auf eine dynamische Festplatte

Um die Aktualisierung auf eine dynamische Festplatte durchzuführen, muss folgendes ausgeführt werden:

- 1. Zur Vermeidung von Datenverlusten im Problemfall sollte eine Datensicherung angefertigt werden
- 2. Mit der rechten Maustaste auf die zu aktualisierende Platte klicken
- 3. Auf " In dynamische Festplatte umwandeln " klicken
- 4. Im Dialogfeld " Aktualisierung auf dynamische Festplatte " auswählen

Wenn die Festplatte, die aktualisiert wird, die Startpartition, Systempartition oder eine aktive Auslagerungsdatei enthält, so muss der Computer neu gestartet werden, um den Aktualisierungsvorgang abzuschließen. Bei der Partitionserstellung oder Formatierung usw. ist dagegen kein Neustart erforderlich.

## Aktualisierungsergebnisse

Bei der Aktualisierung werden alle auf der Basisfestplatte vorhandenen Partitionen zu Datenträgern. In der folgenden Tabelle werden die Ergebnisse einer Aktualisierung beschrieben.

Organisation der Basisfestplatte (vor der Aktualisierung)	Organisation der dynamischen Festplatte (nach der Aktualisierung)
System- und Startpartition	Einfache Datenträger
Primäre Partition	Einfache Datenträger
Erweiterte Partition	Alle logischen Laufwerke werden zu Einfachen Datenträgern, und der gesamte freie Speicherplatz wird zu nicht zugeordnetem Speicherplatz.
<b>Datenträgersatz</b> aus früheren Windows NT-Versionen (in Win2000 nicht mehr verfügbar)	Übergreifender Datenträger
Stripeset aus früheren Windows NT-Versionen (in Win2000 nicht mehr verfügbar)	Stripesetdatenträger
Spiegelsatz aus früheren Windows NT-Versionen (in Win2000 nicht mehr verfügbar)	Gespiegelter Datenträger
Stripeset mit Parität aus früheren Windows NT-Versionen (in Win2000 nicht mehr verfügbar)	RAID-5-Datenträger

# Zurückkonvertieren in eine Basisfestplatte

Prinzipiell ist die Rückkonvertierung einer dynamischen Festplatte in eine Basisfestplatte möglich. Allerdings bleiben dabei weder die Datenträgerstruktur, noch die Daten auf der Festplatte erhalten.

Die Rückkonvertierung kann folgendermaßen durchgeführt werden:

- 1. Datenträgerverwaltung aufrufen
- 2. Alle Daten und Datenträger auf der Platte löschen
- 3. Mit der rechten Maustaste auf die zu konvertierende Platte klicken
- 4. "In eine Basisfestplatte zurückkonvertieren " anklicken

### Erstellen von einfachen Datenträgern

Ein einfacher Datenträger:

- Enthält Speicherplatz auf einer einzelnen Festplatte
- Hat weniger Beschränkungen als eine Basisfestplattenpartition
- Kann die NTFS-, FAT-, oder FAT32-Dateisysteme verwenden
- Kann gespiegelt werden, um Fehlertoleranz bereitzustellen (vorher ist er nicht Fehlertolerant)
- Wird durch die Verwendung des Assistenten zum Erstellen von Datenträgern erstellt

Erstellt wird ein einfacher Datenträger in der Datenträgerverwaltung, indem man mit der rechten Maustaste auf die dynamische Platte klickt und die Option **Datenträger erstellen** auswählt. Danach startet der Assistent  $\rightarrow$  Weiter klicken. **Einfacher Datenträger** auswählen und den Anweisungen auf dem Bildschirm folgen.

### Erweitern einfacher Datenträger

Um einen Datenträger zu erweitern, muss in der Datenträgerverwaltung der zu erweiternde, einfache Datenträger mit der rechten Maustaste angeklickt werden. Danach auf " **Datenträger erweitern** " klicken und den Anweisungen folgen.

Das Erweitern kann nur ausgeführt werden, wenn:

- der Datenträger unter NTFS formatiert ist
- der Datenträger ursprünglich auf einer dynamischen Festplatte erstellt wurde

<u>Wichtig:</u> Wurde der Datenträger zuerst auf einer Basisfestplatte erstellt und anschließend in eine dynamische Festplatte konvertiert, so kann diese nicht erweitert werden.

# Reparieren von Partitionen und Datenträgern

Bei einer Beschädigung der Festplatte, eine Unterbrechung der Stromzufuhr, oder einer Verbindungsunterbrechung wird die Platte OFFLINE geschalten. Um diese wieder zu reparieren oder zu reaktivieren, muss in der Datenträgerverwaltung folgendes ausgeführt werden:

- 1. Partition oder Datenträger, der als fehlend oder offline markiert ist, mit der rechten Maustaste anklicken
- 2. Auf " Festplatte reaktivieren " klicken

Anschließend sollte diese Platte wieder als ONLINE markiert sein.

### Löschen von Partitionen und Datenträgern

Alle Partitionen von Basisfestplatten und Datenträger von dynamischen Platten können gelöscht werden.

Ausnahmen: Systempartition oder Systemdatenträger

Startpartition oder Startdatenträger

Partitionen oder Datenträger mit einer aktiven

Auslagerungsdatei.

Achtung: zuerst müssen alle logischen Laufwerke und anderen Datenträger ge-

löscht werden, bevor das Löschen erweiterter Partition bzw.

Datenträger möglich ist.

### Hinzufügen von Festplatten von anderen Computern

Wenn eine Festplatte von einem Computer zu einem anderen Computer übertragen wird, so importiert Windows 2000 in den meisten Fällen automatisch eine Festplatte, die Daten enthält. Wird der Status **FREMD** angezeigt, so kann durch einen Klick mit der rechten Maustaste unter dem Punkt " **Fremde Festplatten importieren** " der Importvorgang richtig durchgeführt werden.

### Importieren unvollständiger Datenträger

Wird der Status eines importierten Datenträgers als **Fehler: Unvollständiger Datenträger** angezeigt, so müssen die verbleibenden Datenträger importiert werden, um den Datenträger zu vervollständigen.

Dies gilt insbesondere für:

- Teile eines übergreifenden Datenträgers oder Stripesetdatenträgers
- RAID-5-Datenträger, wenn zwei oder mehr Platten nicht importiert wurden

Wird der Status **Fehlerhafte Redundanz** angezeigt, so ist folgendes vorgefallen:

- es wurde ein gespiegelter Datenträger importiert (der andere Teil fehlt)
- es wurde ein RAID-5-Datenträger importiert (die restlichen Platten fehlen)

Der Zugriff auf die Daten der Festplatten ist möglich, jedoch ist die Redundanz verloren gegangen.

<u>Abhilfe:</u> Verbleibende Festplatten importieren, um den Datenträger zu vervollständigen (anschließend sind die Datenträger wieder Fehlerredundant)!

### Verwalten von Laufwerksbuchstaben

Häufig ist es sinnvoll, Wechselmedien einen Laufwerksbuchstaben zuzuweisen, damit diese sofort <u>nach</u> den permanenten Partitionen und Datenträgern auf dem Computer im Explorer aufgeführt werden.

### Verwalten von Laufwerkspfaden

Ein neues Feature von Windows2000 ist die Verwendung der Datenträgerverwaltung, um ein lokales Laufwerk in einen beliebigen leeren Ordner, statt mit einem Laufwerksbuchstaben auf einem lokalen NTFS - Datenträger bereitzustellen. Dies kann unter anderem dann sinnvoll sein, um einen Druckerpool in ein leeres Verzeichnis auszulagern. (siehe Kapitel 10)

### Remoteverwaltung von Festplatten

In einem Windows 2000 Netzwerk kann eine Remoteverwaltung von Festplatten eines Computers von einem anderen Computer aus ausgeführt werden. Folgende Kriterien müssen für die Remoteverwaltung erfüllt sein:

- Beide Computer müssen Mitglieder derselben Domäne oder Arbeitsgruppe sein
- Das Benutzerkonto, mit dem man sich anmeldet, muss ein Mitglied der Gruppe Administratoren oder Serveroperatoren auf dem Remotecomputer sein

Die Remoteverwaltung wird mit Hilfe der Microsoft Management Console (Ausführen → mmc → im Menü Konsole → Snap-In hinzufügen/entfernen → Hinzufügen → in der Liste der Snap-Ins Datenträgerverwaltung wählen und auf Hinzufügen klicken) ausgeführt.

Die Datenträgerverwaltung auf dem lokalen Computer ermöglicht nur das Verwalten **lokaler Datenträger**. Wenn Datenträger eines anderen Computers verwaltet werden sollen, muss man eine neue Konsole mit Snap-Ins für das Verwalten einer Festplatte auf einem Remotecomputer erstellen.

 Auf anderer Computer klicken, den Namen des Remotecomputers eingeben und auf Fertigstellen klicken

## <u>Defragmentierung von Partitionen</u>

Zum Starten des Defragmentierungsprogramms muss folgendes ausgeführt werden:

#### Start → Programme → Zubehör → Systemprogramme → Defragmentierung

Mit der Überprüfen wird festgestellt, ob der Datenträger fragmentiert ist oder nicht. Nach der Überprüfung erscheint eine Meldung, in der empfohlen wird, die Partition zu defragmentieren oder nicht.

# Unterrichtseinheit 13

### Konfigurieren einer unterbrechungsfreien Stromversorgung

Die Konfiguration erfolgt unter:

#### Start → Einstellungen → Systemsteuerung → Energieoptionen → USV

### Implementieren von Fehlertoleranz mit Hilfe von RAID

#### 1. RAID Implementierungen

Zum Implementieren der RAID Fehlertoleranz unter Windows 2000 gibt es zwei Optionen: eine Software- oder eine Hardwareimplementierung

Vorraussetzung: Windows 2000 Server

#### 2. Softwareimplementierung von RAID

Bei einer Softwareimplementierung von RAID stellt das Betriebssystem einen Mechanismus zum Sicherstellen der Datenredundanz bereit.

#### Folgende RAID – Level werden softwaremäßig von W2K Server unterstützt:

#### RAID 0

RAID 0 wird auch als **Datenträgerstriping** bezeichnet. Die Daten auf einem Datenträger werden in einem Stripeset auf mindestens zwei physischen Datenträgern gespeichert.

Vorteil: erhöhte Lese- und Schreibgeschwindigkeit durch gleichzeitigen Zugriff

auf mehrere Festplatten

Nachteil: keine Fehlertoleranz, keine Ausfallsicherheit, nur unter NTFS möglich

#### RAID 1

RAID 1 wird auch als Festplattenspiegelung bezeichnet. Dabei werden Daten gleichzeitig auf zwei Festplatten geschrieben. Falls eine Festplatte ausfällt, können die Daten der zweiten Festplatte verwendet werden. Allerdings werden nur 50% des insgesamt verfügbaren Speicherplatzes verwendet.

Vorteil: Wiederherstellung verlorengegangener Daten möglich

Kosten pro MB höher, da nur die Hälfte des Speicherplatzes verwendet Nachteile:

> wird. Schreibleistung etwas langsamer, da Daten auf beide Datenträger geschrieben werden müssen. Dieser Nachteil kann jedoch umgangen werden, wenn jede der Fest-platten über einen eigenen Controller an-

gesprochen wird (Festplattenduplizierung).

#### RAID 5

RAID 5 wird auch als **Stripeset mit Parität** bezeichnet. Stripesets mit Parität sind normalen Stripesets sehr ähnlich. Sie enthalten jedoch zusätzlich einen Mechanismus zur Fehlertoleranz. **Jede** Festplatte enthält in regelmäßigen Abständen Paritätsinformationen, aus denen beim Ausfall einer <u>beliebigen</u> Platte die verlorenen Daten rekonstruiert werden können.

Vorteil: erhöhte Lesegeschwindigkeit

Nachteile: Systempartitionen können nicht geschützt werden, Schreiben dauert

länger als bei gespiegelten Datenträgern

**Wichtig:** Bei Softwareimplementierungen von RAID ist die Rechenzeit etwas höher als bei einer Hardwarelösung. Weiterhin steht **keine** Fehlertoleranz <u>nach</u> einem Fehler zur Verfügung, bis dieser nicht behoben ist. Wenn in der Zwischenzeit noch ein zweiter Fehler auftritt, so müssen die Daten von einer Sicherheitskopie wiederhergestellt werden.

#### Hardwareimplementierung von RAID

Bei einer Hardwareimplementierung von RAID bearbeitet die Schnittstelle des Festplattencontrollers die Erstellung und erneute Erzeugung von redundanten Informationen. Die RAID Ebene hängt dabei vom Hersteller der Hardware ab.

Vorteile: schneller im Gegensatz zur Softwareimplementierung, Austausch defekter

Datenträger im laufenden Betrieb möglich (Hot Swapping)

Nachteil: sehr teuer

## Gespiegelte Datenträger

Bei gespiegelten Datenträgern werden die Fehlertoleranztreiber von Windows 2000 Server (**Ftdisk.sys**) verwendet , um die Daten gleichzeitig auf beide Datenträger zu schreiben.

**Anmerkung:** Ein gespiegelter Datenträger kann beliebige Partitionen (auch die Start- oder Systempartition) enthalten. Allerdings müssen dann beide Festplatten unter Windows 2000 als dynamische Datenträger konfiguriert werden.

#### Merkmale gespiegelter Datenträger:

- Unter FAT und NTFS möglich
- System- oder Startpartitionen können ebenfalls geschützt werden
- Zwei Festplatten sind erforderlich
- **50** % Speicherausnutzung ( dadurch teuerer )
- Lese und Schreibleistung ist gut
- Im Vergleich zu RAID 5 verbrauchen gespiegelte Datenträger weniger Systemspeicher

### RAID 5 Datenträger

#### Merkmale von RAID 5 Datenträgern

RAID 5 Datenträger weisen gegenüber gespiegelten Datenträgern einen Kostenvorteil auf, da die Verwendung der Festplatte optimiert wurde. Gesamter Speicherplatz des RAID 5 Datenträgers abzüglich <u>eines</u> Datenträgers lautet die Gleichung zum Bestimmen des Speicherplatzes, der vom RAID-5-Datenträger verwendet wird. Je mehr Festplatten im RAID-5-Datenträger zur Verfügung stehen, desto geringer sind die Kosten des redundanten Datenstripe.

Die folgende Tabelle zeigt, wie der für ein Datenstripe erforderliche Speicherplatz durch das Hinzufügen von **2-GB**-Festplatten zum RAID-5-Datenträger vermindert wird.

Festplatten- Anzahl	Verwendeter Festplattenspeicher	Verfügbarer Festplattenspeicher	Redundanz
3	6 GB	4 GB	33 % (Parität)
4	8 GB	6 GB	25 % (Parität)
5	10 GB	8 GB	20 % (Parität)

#### Vorteile von RAID-5-Datenträgern

- Die Datenträger unterstützen FAT und NTFS
- Im Vergleich zu gespiegelten Datenträgern sind die Kosten pro MB geringer
- Schreibleistung mittelmäßig, aber Leseleistung ist sehr gut

#### Nachteile von RAID-5-Datenträgern

- System- oder Startpartitionen k\u00f6nnen nicht gesch\u00fctzt werden
- Es sind mindestens **drei** Festplatten erforderlich
- Mehr Systemspeicher ist erforderlich

Wiederherstellen eines fehlerhaften gespiegelten Datenträgers auf einer Festplatte mit dem Status "Online (Fehler)"

# Start → Einstellungen → Systemsteuerung → Verwaltung → Computerverwaltung → Datenträgerverwaltung

Mit der rechten Maustaste erst auf die fehlerhafte Festplatte, danach auf **Festplatte reaktivieren** klicken. Als Status des Datenträgers sollte nun wieder **Fehlerfrei** angegeben sein und der gespiegelte Datenträger **automatisch** neu erzeugt werden.

**Wichtig:** Wenn der Datenträger nicht repariert werden kann, wird möglicherweise im Menü nur die Option **Löschen** angezeigt. In diesem Fall muss die Platte ersetzt werden. Mit dem nächsten Punkt fortfahren.

## <u>Ersetzen einer Festplatte und Erstellen eines neuen gespiegelten</u> Datenträgers

Zum Erstellen eines neuen gespiegelten Datenträgers, nach vergeblichen Versuch, die Festplatte mit dem Status "Online(Fehler)" zu reaktivieren, müssen folgende Schritte durchgeführt werden:

- 1. In der **Datenträgerverwaltung** auf die fehlerhafte Platte mit der rechten Maustaste klicken und dann auf **Spiegelung entfernen**
- 2. Im Dialogfeld **Spiegelung entfernen** zuerst auf die fehlerhafte Festplatte und anschließend auf **Spiegelung entfernen** klicken
- 3. Mit der rechten Maustaste auf den zu spiegelnden Datenträger und anschließend auf **Spiegelung hinzufügen** klicken
- 4. Die zweite Festplatte im gespiegelten Datenträger auswählen und anschließend auf **Spiegelung hinzufügen** klicken

## <u>Wiederherstellen eines fehlerhaften RAID-5-Datenträgers auf einer</u> Festplatte mit dem Status "Offline" oder "Fehlend"

Hier wird genauso wie bei gespiegelten Datenträgern verfahren. Führt dies ebenfalls zu keinem Ergebnis, muss mit folgendem Schritt fortfahren werden:

Ersetzen einer Festplatte und erneutes Erzeugen eines RAID-5-Datenträgers

Zum erneuten Erzeugen eines RAID-5-Datenträgers mit Hilfe einer anderen neuen Festplatte müssen folgende Schritte ausgeführt werden:

- 1. In der **Datenträgerverwaltung** mit der rechten Maustaste auf den RAID-5-Datenträger auf der fehlerhaften Festplatte, und dann auf **Datenträger reparieren** klicken.
- 2. Im Dialogfeld **RAID-5-Datenträger reparieren** die Festplatte auswählen, durch die die fehlerhafte Festplatte im RAID-5-Datenträger ersetzt wird und anschließend auf **O.K.** klicken.

# Übersicht über Datensicherung und -wiederherstellung

Um Daten zu sichern, kann das in Windows 2000 implementierte Sicherungsprogramm verwendet werden.

Pfad : Start → Programme → Zubehör → Systemprogramme → Sicherung

Schnellere Variante : Start → Ausführen → ntbackup.exe

Anmerkung: Mit Hilfe von Windows Backup wird auch die Notfalldiskette erstellt.

### Berechtigungen und Benutzerrechte

Zum erfolgreichen Sichern und Wiederherstellen von Daten auf einem Computer unter Windows 2000 muss man über die entsprechenden Berechtigungen und Benutzerrechte verfügen, die in der folgenden Liste beschrieben sind.

- Alle Benutzer können ihre eigenen Dateien und alle Dateien, für die sie über die Leseberechtigung verfügen, sichern
- Alle Benutzer können Dateien und Ordner wiederherstellen, für die sie über eine Schreibberechtigung verfügen
- Administratoren, Sicherungsoperatoren und Serveroperatoren können alle Dateien - unabhängig derer Berechtigungen - sichern und wiederherstellen, da Mitglieder dieser Gruppen standardmäßig über die Berechtigungen Dateien und Verzeichnisse sichern und Dateien und Verzeichnisse wiederherstellen verfügen.

### Sicherungsarten

Art	Sicherungsumfang
Normale Sicherung	Alle ausgewählten Dateien und Ordner. Markierungen (Archivattribut) werden gelöscht, aber es wird nicht nach Markierungen gesucht.(schnellste Variante) Archivattribut gesetzt: Eine Änderung seit dem letzten Backup ist eingetreten Archivattribut nicht gesetzt: es ist ein aktuelles Backup vorhanden
Kopie- Sicherung	Wie Normale Sicherung, nur werden die Markierungen nicht gelöscht
Differenzielle Sicherung	Nur ausgewählte Dateien und Ordner, die seit der letzten Sicherung geändert wurden. Die Markierungen werden dabei nicht gelöscht.
Inkrementelle Sicherung	Wie Differenzielle Sicherung, nur werden hier die Markierungen gelöscht.
Tägliche	Ausgewählte Dateien und Ordner, die im Verlauf des Tages geändert wurden

# Sichern der Systemstatusdaten

Die Systemstatusdaten enthalten Informationen zum Wiederherstellen des Betriebssystems in den Zustand vor dem Fehler. Die Systemstatusdaten schließen die folgenden Systemkomponenten ein:

- Registrierung
- Registrierungsdatenbank für Klassen der Komponentendienste
- Systemstartdateien
- Zertifikatsdienste-Datenbank
- Verzeichnisdienst Active Directory<sup>TM</sup>
- Ordner Sysvol

**Anmerkung:** Einzelne Komponenten können nicht gesichert werden.

Nicht jede Variante von Windows 2000 sichert alle oben aufgeführte Systemstatusdaten. In der folgenden Tabelle wird dies genauer erläutert:

Komponenten	DC	Server	Professional
Registrierung	Х	X	X
Regisrierungsdatenbank für CS	Х	X	X
Systemstartdateien	Х	Х	X
Zerifikatsdienste-Datenbank	Х	X	
Active Directory	Х		
Ordner "Sysvol"	Х		

## Verwenden der Wiederherstellungstools für Notfälle

#### Starten eines Computers mit Hilfe der erweiterten Startoptionen

Die erweiterten Startoptionen erreicht man nach der Auswahl des Betriebssystems durch drücken der Taste F8.

Folgende Optionen stehen zur Auswahl:

Abgesicherter Modus	Lädt die wichtigsten Geräte und Treiber
Abgesicherter Modus mit Netzwerktreibern	Lädt Optionen des abgesicherten Modus, von Netzwerkdiensten und Treibern
Abgesicherter Modus mit Eingabeaufforderung	Lädt Optionen des abgesicherten Modus, statt der grafischen Ober- fläche wird jedoch die Eingabeaufforderung angezeigt
Startprotokollierung aktivieren	Protokolliert das Laden und die Initialisierung der Treiber und Dienste (die Datei heißt <b>Ntblog.txt</b> )
VGA-Modus aktivieren	Lädt den Basis VGA-Treiber
Letzte als funktionierend bekannte Konfiguration	Verwendet die letzte als funktionierend bekannte Konfiguration zum Starten des Computers
Verzeichnisdienstwiederh.	Ermöglicht die Wiederherstellung von Active Directory auf DC
Debugmodus	Aktiviert Debugging

Anmerkung: Die Optionen Abgesicherter Modus und Abgesicherter Modus mit Eingabeaufforderung stehen auf einem Domänencontroller zwar zur Verfügung, jedoch sind in diesen Fällen keine Active Directory Dienste verfügbar.

## <u>Wiederherstellen eines Computers mit Hilfe der Wiederherstellungs-</u> konsole

Die Wiederherstellungskonsole wird nicht standardmäßig installiert und muss deswegen nachträglich eingerichtet werden:

- Windows 2000 CD einlegen
- Eingabeaufforderung starten
- Auf der CD in das Verzeichnis i386 wechseln
- Winnt32 /cdmcons eingeben

Die Wiederherstellungskonsole steht nach dem nächsten Neustart des Computers in der Betriebssystemsauswahlphase zur Verfügung und kann nur mit dem **Administratoraccount** ausgeführt werden.

# <u>Wiederherstellen eines Computers mit Hilfe des Notfallreparaturvorgangs</u>

#### Erstellen einer Notfalldiskette

Eine Notfalldiskette kann mit dem Sicherungsprogramm Ntbackup.exe erstellt werde.

#### Verwenden des Notfallreparaturvorgangs

Die Informationen für den Reparaturvorgang stehen im Ordner %Systemroot%Repair

Nachdem der Computer neu gestartet wurde, muss das Installationsprogramm ausgeführt werden. In der darauffolgenden Auswahl **vorhandene Installation reparieren** auswählen und **R** drücken.

In der nächste Auswahl **Notfallreparaturvorgang** wählen und wieder **R** drücken. Als Nächstes den Reparaturtyp (**schnelle oder manuelle** Reparatur) wählen und die Notfalldiskette einlegen. Als letztes den Vorgang starten. War dieser dann erfolgreich, so wird das System neu gestartet und es sollte wieder einwandfrei arbeiten.

Ein kleiner Leitfaden zur Behebung von Fehlern ihrem Schweregrad entsprechend:

Bei kleinen Fehlern: F8 → letzte als funktionierend bekannte Konfiguration

F8 → abgesicherter Modus

Bei schweren Fehlern: Wiederherstellungskonsole

Als letzte Möglichkeit: Notfallreparatur mit Hilfe des Installationsprogramms

# **Unterrichtseinheit 14**

## Einführung in die Terminaldienste

Die Terminaldienste ermöglichen **Mehrbenutzerzugriff** auf Windows 2000. Da alle Anwendungen auf dem Server ausgeführt werden und auch die gesamte Datenverarbeitung auf dem Server erfolgt, benötigen Clients weder große Mengen an Arbeitsspeicher, noch eine hohe Verarbeitungsleistung. Es gibt **zwei** Betriebsmodi, in denen ein Terminalserver arbeiten kann:

#### Remoteverwaltung und Anwendungsserver.

### Funktionsweise der Terminaldienste

Die Terminaldienste bestehen aus drei Teilen:

■ Terminalserver: Er verwaltet die Computerressourcen für alle Clientsitzun-

gen und stellt allen angemeldeten Benutzern eine eigene,

einzigartige Umgebung zur Verfügung.

Client : Die Terminalsitzung wird als Fenster in der lokalen Desk-

topumgebung geöffnet. Der Remotedesktop des Servers wird in diesem Fenster ausgeführt. Diese Clients werden

oft auch Thin Clients genannt.

Remote Desktop Protocol:
RDP ist das verwendete Protokoll, welches

auf der Anwendungsebene operiert und für den Transport über das Netzwerk auf TCP/IP aufsetzt. Es basiert auf dem Standard T.120 der ITU (International Telecommunication

Union)

## <u>Benutzerumgebungen</u>

Um den Clients den Zugriff auf den Terminalserver zu ermöglichen, muss zuerst der **Terminaldienstclient** auf dem Clientcomputer installiert werden. Erst jetzt kann der Client Verbindung zum Terminalserver aufnehmen, indem er unter **Start** → **Programme** den Terminaldienstclient und anschließend einen verfügbaren Terminalserver auswählt und auf Verbinden klickt.

#### Features und Vorteile

- Zentralisierte Bereitstellung von Spartenanwendungen
- Zugriff auf den Windows 2000 Desktop
- Erweiterte Verwaltungs- und Supportmöglichkeiten

### Zentralisierte Bereitstellung von Spartenanwendungen

Die Hardware für die Clients ist kostengünstiger, da der Client nur über ausreichend Leistung verfügen muss, um die Verbindung zum Server herstellen zu können. Weiterhin ist der Zugriff auf aktualisierte oder neue Software einfacher, da der Administrator nicht auf jedem Desktopcomputer, sondern nur einmal auf dem Server die Anwendung installieren muss.

#### **Zugriff auf den Windows 2000 Desktop**

**Anmerkung:** Wenn das Add-On MetaFrame von Citrix installiert ist, können auch nicht Windows-Clients (Unix-Clients) die Verbindung zu den Terminaldiensten herstellen.

#### Vorteile:

- Ältere Geräte können weiter verwendet werden
- Ersetzen von textbasierten Terminals
- Erhöhte Sicherheit und Zuverlässigkeit durch Verschlüsselung

Es stehen **drei** Verschlüsselungsebenen zur Verfügung: niedrig, mittel, hoch. Alle Verschlüsselungsebenen verwenden die standardmäßige **RSA-Verschlüsselung** (**Rivest-Shamir-Adleman**) RC4.

#### Erweiterte Verwaltungs- und Supportmöglichkeiten

Remoteverwaltung: neues Feature, das dem Administrator eine Re-

moteverwaltung von Microsoft Backoffice Servern

und Domänencontrollern ermöglicht

■ Remotesupport: bietet dem Administrator die Möglichkeit, bei akti-

vierter Remotesteuerung einem am Terminalserver angemeldeten Benutzer von einer anderen Client-

sitzung aus zu (ver)folgen

## Identifizieren der Clientanwendungen

Folgende Anwendungen können auf dem Terminalserver installiert werden:

- Windows-basierte Anwendungen (32 Bit)
- MS-DOS-Anwendungen (16Bit)
- Andere anwendungsbezogene Aspekte: Einzelbenutzeranwendungen, Anwendungen, für die besondere Hardware benötigt wird, benutzerdefinierte Anwendungen

#### Windows-basierte Anwendungen

Windows-basierte 32-Bit-Anwendungen arbeiten effizienter als 16-Bit-Anwendungen, da sie die Vorteile von 32-Bit-Hardware und 32-Bit-Betriebssystemen in vollem Umfang nutzen können. Durch das Ausführen von 16-Bit-Anwendungen auf einem Terminalserver kann die **Anzahl der** 

Benutzer, die prozessorseitig unterstützt wird, um 40 % verringert und die pro Benutzer benötigte Speichermenge um 50 % erhöht werden.

#### - MS-DOS-Anwendungen

Da MS-DOS basierte Anwendungen nicht für das Ausführen in einer Mehrbenutzerumgebung entworfen wurden, kann das Ausführen dieser auf einem Terminalserver die Systemleistung mit Leerlaufprozessen negativ beeinflussen. (MS-DOS-Programme warten die meiste Zeit auf Eingaben!!!)

Betriebssystem	RAM	Prozessor	Grafikkarte
Windows 2000	32 MB	Pentium	VGA
WinNT 3.51 oder 4.0	16 MB	486	VGA
Windows 98	16 MB	486	VGA
Windows 95	16 MB	386	VGA
Windows 3.11	16 MB	386	VGA
Windows CE, Handheld	Hersteller	Hersteller	Hersteller

# Bestimmen der Serverkonfiguration für die Benutzerunterstützung

Folgenden Empfehlungen müssen unbedingt <u>vor</u> dem Installieren der Terminaldienste im Hinblick auf die Systemkonfiguration beachtet werden:

#### Computerausstattung:

Servertyp: Installation nur auf einem Mitgliedsserver, nicht auf

einem **Domänencontroller**, da die Leistung aufgrund des zusätzlichen Speicherbedarfs, Netzwerkverkehrs und Pro-

zessorzeit negativ beeinflusst werden

Arbeitsspeicher: Für jede Terminalsitzung benötigt ein Terminalserver zu-

sätzlichen Arbeitsspeicher von 4-10 MB

Dateisystem: es wird eine NTFS-Partition empfohlen

#### Peripheriegeräte:

■ **Festplatten:** Um die beste Leistung zu erzielen → SCSI RAID Controller

Netzwerkadapter: Ein Netzwerkadapter mit hoher Leistung; die Verwendung

mehrere Netzwerkadapter kann den Netzwerkdurchsatz

erheblich erhöhen.

## <u>Benutzereigenschaften</u>

Die Verwendungsmuster von Computerbenutzern können signifikante Auswirkungen auf die Leistung der Terminaldienste haben. Bei den Leistungstests von Microsoft wird das Benutzerverhalten in den folgenden drei Kategorien simuliert:

■ Dateneingabe: Benutzer führen eine einzige Anwendung aus, die

sie für Dateneingabe verwenden (z.B. Geschäftsan-

wendungen)

• Strukturierte Aufgaben: Benutzer führen ein oder zwei Anwendungen

gleichzeitig aus. Meist sind dies Anwendungen, deren Datenverarbeitungsanforderungen nicht sehr anspruchsvoll sind (z.B. Word). Die Anwendungen werden häufig geöffnet und geschlossen und die

Eingabegeschwindigkeit ist relativ hoch.

• Wissen: Benutzer führen drei oder mehr Anwendungen

gleichzeitig aus. Die Anwendungen sind im allgemeinen geöffnet und ihre Datenverarbeitungsanforderungen an das System sehr hoch (z.B. Daten-

bankabfragen)

### <u>Identifizieren der Lizenzierungsanforderungen</u>

Für die Terminaldienste ist es erforderlich, dass jedes Gerät, das eine Terminaldienstsitzung initiiert, entweder mit einer Windows 2000 Lizenz, oder mit einer Clientzugriffslizenz (Client Access License, CAL) lizenziert ist. Für die Terminaldienste wird darüber hinaus auch ein Lizenzserver benötigt, auf dem der Dienst für die Terminaldienstlizenzierung aktiviert ist.

#### Richtlinien für einen Lizenzserver

Der Dienst für die Terminaldienstlizenzierung ist ein Komponentendienst von **Windows 2000 Server**. Die Lizenzierung ist nur dann erforderlich, wenn der Terminalserver im **Anwendungsservermodus** läuft. Ein Lizenzserver kann mehrere Terminalserver unterstützen.

In einer **Windows 2000 Domäne** muss der Lizenzserver ein **Domänencontroller** sein, wohingegen in einer **Arbeitsgruppe oder Domäne unter Windows NT 4.0** der Lizenzserver auf einem **beliebigen Peerserver** bereitgestellt werden kann. Die Terminaldienstlizenzierung verwaltet jedoch <u>keine</u> Terminalserver unter Windows NT 4.0.

Für die Terminaldienstlizenzierung werden pro **6000** ausgestellten Clientlizenzen etwa **5 MB** Festplattenspeicher benötigt. Die Speicherverwendung liegt, ob im Leerlauf oder aktiv, unter **10 MB** RAM.

### Arten von Clientlizenzen

Der Lizenzserver verwaltet folgende Arten von Lizenzen:

- Clientzugriffslizenzen für Terminaldienste: für Nicht-W2K-Clients
- Internetconnector-Lizenzen: anonyme Verwendung über das Internet

Integrierte Lizenzen: für Clients unter Windows 2000

■ Temporäre Lizenzen: wird vom Terminalserver eine Lizenz angefordert,

aber der Lizenzserver keine zu vergeben hat, stellt

dieser eine temporäre Lizenz aus

#### Installieren der Terminaldienste

# Start → Einstellungen → Systemsteuerung → Software → Windows-Komponenten hinzufügen → Terminaldienste

Es muss der Modus, in dem der Terminalserver betrieben werden soll ausgewählt werden. Die folgenden zwei Möglichkeiten stehen zur Auswahl:

- Remoteverwaltung
- Anwendungsserver

**Wichtig:** Nach der Installation sucht der Terminalserver nach einem Lizenzserver. Die Terminaldienste arbeiten **90 Tage** ohne Lizenzserver. Nach 90 Tagen wird das Herstellen einer Verbindung von einem nicht lizenzierten Client zum Terminalserver nicht mehr zugelassen, falls kein Lizenzserver zur Verfügung steht.

Durch die Installation der Terminaldienste werden mehrere Elemente zum Menü **Verwaltung** hinzugefügt:

Terminaldienste-Clientinstallation erstellt Disketten zum Installieren der Terminaldienste

und der Clientsoftware

Terminaldienstekonfiguration verwaltet die Protokollkonfiguration und die Server-

stellungen für die Terminaldienste

Terminaldiensteverwaltung verwaltet und überwacht Sitzungen und Vorgänge auf

dem Terminalserver

Standardmäßig wird die Terminaldienste-Clientsoftware im Ordner %Systemroot%\System32\Clients\Tsclient installiert.

Falls mehrere Terminalserver bereitgestellt werden, allerdings die Clientsoftware nicht installiert werden soll, wählt man **Terminaldienste** aus, klickt auf **Details** und deaktiviert das Kontrollkästchen **Clienterstellungsdateien**.

### Konfigurieren des Benutzerzugriffs

Computerverwaltung → unter lokale Benutzer und Gruppen auf den gewünschten Benutzer doppelklicken → auf der Registerkarte Terminaldiensteprofile das Kontrollkästchen Terminalserver-Anmeldung zulassen aktivieren, bzw. deaktivieren.

Auf dieser Registerkarte können auch die Basisverzeichnisse und Ordner für die Terminalbenutzerprofile angegeben werden.

## Erstellen von Clientinstallationsdisketten

#### Start → Programme → Verwaltung → Terminaldienste-Clientinstallation

Hier muss der Typ für die Clientsoftware ausgewählt werden:

- Terminaldienste für 16-Bit Windows (erfordert 4 Disketten)
- Terminaldienste für 32-Bit-x86 Windows (erfordert 2 Disketten)

Nach dem Einlegen der Diskette werden die Dateien kopiert.

### Downloaden der Clientsoftware über das Netzwerk

Die Quelldateien für den Terminaldiensteclient befinden sich im Ordner: %Systemroot%\System32\Clients\Tsclient
Der Ordner Tsclient enthält die Unterordner Net, Win16 und Win32

## Herstellen einer Verbindung zu einem Terminalserver

Starten des **Terminaldiensteclients** → Servername oder IP-Adresse angeben → Auflösung einstellen → **Datenkomprimierung** aktivieren oder deaktivieren → **Bitmaps zwischenspeichern** aktivieren oder deaktivieren → **Verbinden** 

Die Option **Datenkomprimierung aktivieren** sollte ausgewählt werden, wenn z.B. ein Modem verwendet wird, oder der Rechner in einem langsamen Netzwerk steht.

Die Option **Bitmaps zwischenspeichern** wird verwendet, um Anzeigeelemente des Desktops im **Iokalen** Cache zu speichern.

## Beenden einer Terminalsitzung

Die Terminaldienste bieten einem Benutzer zwei Optionen für das Beenden einer Terminalsitzung an:

Trennen einer Sitzung beim Trennen einer Sitzung wird diese auf

dem Server weiter ausgeführt

Abmelden einer Sitzung mit dem Abmelden wird die Sitzung auf dem

Server beendet

Es gibt zwei Möglichkeiten, die Dialogfelder zum Abmelden und Trennen der Sitzungen zu erreichen:

Start → Herunterfahren → Dialogfeld Windows herunterfahren → Abmelden oder Trennen

#### **ODER**

Tastenkombination STRG+ALT+ENDE → Herunterfahren → Abmelden oder Trennen

**Anmerkung:** Es ist empfehlenswert, dass sich die Benutzer von ihren Sitzungen am Terminalserver **abmelden**, um so **Arbeitsspeicher und Ressourcen** des Servers anderen Sitzungen zur Verfügung zu stellen.

## Installation von Anwendungen auf einem Terminalserver

Es gibt zwei Methoden zum Installieren von Anwendungen auf einem Terminalserver:

- 1. Die Option **Software** in der Systemsteuerung (führt **change user** automatisch aus)
- 2. Der Befehl **change user** in der Eingabeaufforderung

Schlägt die Installation mit der Option **Software** fehl, kann der Befehl **change user** auch manuell ausgeführt werden.

Folgende Schritte sind dafür erforderlich:

- 1. als **Administrator** am Terminalserver anmelden
- 2. in der Eingabeaufforderung **change user /install** eingeben
- 3. installieren der Anwendung auf einem lokalen Laufwerk
- 4. nach Abschluss der Installation **change user /execute** eingeben

# Unterrichtseinheit 15

#### Bereitstellen von Windows 2000

Es gibt vier verschiedene Möglichkeiten, um Windows 2000 auf einem Rechner bereitzustellen. In der folgenden Tabellen werden diese genau erläutert:

Installationsmethode	Vorteil	Nachteil
CD	einfach und schnell	muss lokal auf <u>jedem</u> Clientcomputer bereitgestellt werden. Der Zugriff auf die CD ist erforderlich.
Netzwerk	der Zugriff ist an jeder beliebigen Stelle im Netzwerk mit den ent- sprechenden Zugriffs- rechten möglich.	Verwendet <b>Speicherplatz</b> auf einem Server. <b>Langsame Installation</b> über WAN. Erfordert die Installation eines freigegebenen Netzwerkordners. Bereitstellung erfolgt lokal für alle Clients.
Festplatten- duplizierung	äußerst effizient und am schnellsten. Der Zugriff ist an jeder beliebigen Stelle im Netz möglich.	verwendet Speicherplatz auf einem Server. Erfordert die Installation eines freigegebenen Netzwerkordners. Verwendet Software von Drittanbietern. Erfordert umfangreiche Vorbereitung. Bereitstellung erfolgt lokal auf jedem Clientcomputer.
Remoteinstallation	kann Remote von einem Server bereitgestellt wer- den.	Erfordert besondere Hardware. Verwendet Speicherplatz auf einem Server. Erfordert die Installation eines freigegebenen Netzwerkordners. Erfordert umfangreiche Vorbereitung.

## Durchführen einer manuellen Installation

Das Installieren von Windows 2000 über eine Netzwerkverbindung ist zwar einfach, es müssen jedoch ein paar Anforderungen erfüllt werden, damit die Installation erfolgreich ist. Diese zusätzlichen Anforderungen umfassen folgendes:

- einen Verteilungsserver, der die Installationsdateien aus dem Ordner i386 auf der Windows 2000 CD enthält
- Netzwerkclientsoftware, mit deren Hilfe der lokale Computer eine Verbindung zum Verteilungsserver herstellen kann
- eine Partition mit mindestens 685 MB (empfohlen: 1 GB oder größer) auf dem lokalen Computer

Nachdem diese Anforderungen erfüllt sind, kann die Netzwerkinstallation durchgeführt werden.

Um eine Netzwerkinstallation zu initiieren, müssen folgende Schritte durchgeführt werden:

- 1. den Computer mit der **Netzwerkclientsoftware** starten
- 2. eine Verbindung zum freigegebenen Ordner **i386** herstellen
- 3. ausführen von **WINNT.EXE** (unter DOS im 16-Bit Modus), bzw. **WINNT32.exe** (von der Windowsoberfläche aus), um eine vorherige Installation zu aktualisieren.

WINNT.EXE, bzw. WINNT32.EXE erstellen den temporären Ordner **\$Win\_nt\$.~Is** und kopieren in diesen entsprechend die Windows Installationsdateien.

## <u>Anpassen von Installationen und Aktualisierungen mit Hilfe von</u> Schaltern

Das Installationsprogramm **WINNT.EXE** wird verwendet, um Windows 2000 ausgehend von einem beliebigen 16-Bit-Betriebssystem (z.B. MS-DOS) zu installieren, wohingegen das Aktualisierungsprogramm **WINNT32.EXE** verwendet wird, um vorhandene Installationen von Windows 98/NT4.0 innerhalb eines 32-Bit-Betriebssystems aus zu aktualisieren.

# <u>Ändern des 16-Bit Installationsprogramms Winnt.exe mit Hilfe von Schaltern</u>

Schalter	Aufgabe
/a	Aktivieren von Optionen für die Eingabehilfen
/e [:Befehl]	Ausführen eines Befehls vor dem abschließenden Teil der Installation
/udf:Kennung[,UDF-Datei]	Ändern der Antwortdatei
/r[:Ordner]	Angeben eines zu installierenden optionalen Ordners
/rx[:Ordner]	Angeben eines zu kopierenden optionalen Ordners
/s[:Quellpfad]	Angeben des Speicherortes der Installationsdateien
/t[:Temporärlaufwerk]	Angeben eines Laufwerkes für die Installation
/u[:Antwortdatei]	Unbeaufsichtigte Installation mit einer Antwortdatei

# Ändern des 32-Bit Installationsprogramms Winnt32.exe mit Hilfe von Schaltern

Schalter	Aufgabe
/copydir:Ordner	Erstellen eines zusätzlichen Ordners (oder /copysource)
/cmd:Befehlszeile	Ausführen eines Befehls vor dem abschließenden Teil der Installation
/cmdcons	Installieren der Dateien für die Wiederherstellungskonsole
/debug[Ebene]:[Dateiname]	Erstellen eines Debugprotokolls auf der angegebenen Ebene
/s:Quellpfad	Angeben des Quellortes der Installationsdateien
/syspart:Laufwerksbuchstabe	Kopieren von Startdateien für das Installationsprogramm auf eine Festplatte, die dann in andere Rechner eingebaut wird.
/tempdrive:[Laufwerksbuchstabe]	Angeben eines Laufwerkes für die Installation
/unattend[Zahl]:[Antwortdatei]	Durchführen einer unbeaufsichtigten Installation mit einer optionalen Antwortdatei
/udf:Kennung[,UDF-Datei]	Installieren mit Hilfe einer UDF-Datei (Uniqeness Database File)

# <u>Installieren von Windows 2000 mit Hilfe des Assistenten für den Installations-Manager</u>

- Erstellen und ändern von Antwortdateien mit Hilfe des Assistenten für den Installationsmanager
- Angeben eindeutiger Computervariationen

Der Assistent für den Installationsmanager automatisiert Installationen von Windows 2000 und bietet Flexibilität, wenn dieses auf Netzwerkcomputern mit unterschiedlichen Konfigurationen installiert werden muss.

#### Verwenden von Antwortdateien und UDF-Dateien

Antwort- und UDF-Dateien werden verwendet, um die **Automatisierung** von **Remote-, bzw. unbeaufsichtigten Installationsvorgängen** zu unterstützen. Dabei gibt die Antwortdatei **allgemeine Informationen** an, welche für <u>alle</u> zu installierenden Computer gleich sind. Die UDF-Datei enthält Informationen, die für einen **bestimmten Computer** im Netzwerk eindeutig sind, wie *z.B. Netzwerkeinstellungen und Computernamen*. Beide Dateien zusammen ermöglichen eine erfolgreiche Remote-, bzw. unbeaufsichtigte Installation.

## Starten des Assistenten für den Installationsmanager

Der Assistent für den Installationsmanager, welcher allerdings nicht standardmäßig mitinstalliert wird, heißt **Setupmgr.exe**. Um den Installationsmanager nutzen zu können, müssen folgende Schritte ausgeführt werden:

- 1. auf der Windows 2000 CD in den Ordner /support/tools wechseln
- 2. die Datei **Deploy.cab** doppelt anklicken
- 3. alle Dateien markieren und mit der **rechten** Maustaste anklicken
- 4. extrahieren wählen und in einen ausgewählten Ordner extrahieren

## Angeben eindeutiger Computervariationen

Dateien für die unbeaufsichtigte Installation werden erstellt, um einen Computer ohne manuelles eingreifen installieren zu können. Müssen viele Computer installiert werden, so kann man für jeden Computer im Netzwerk eindeutige Informationen angeben. Einige Konfigurationsvariablen, wie z.B. Computername, IP-Adresse... müssen für jeden Computer im Netzwerk eindeutig sein. Zum vollständigen Automatisieren einer Installation kann entweder für jeden Computer eine eigene Antwortdatei, oder UDF-Dateien verwendet werden.

Eine UDF-Datei kann über mehrere Computernamen, welche jeweils eine andere Konfiguration aufweisen, verfügen.

Werden mehrere Computernamen im Assistenten für den Installationsmanager angegeben, so erstellt das Programm die folgenden Dateien :

Standarddateiname	Zweck
Unattend.txt	gibt Installationsinformationen an die für <b>alle</b> Computer gleich sind, sowie die Computernamen der einzelnen Computer
Unattend.udf	stimmt mit den Computernamen überein, die in der Datei Unattend.txt für SID`s (Security Identifier) angegeben sind
Unattend.bat	stellt eine Batchdatei bereit, mit der die Verwendung der Schalter /u für Winnt.exe, bzw. /unattend für Winnt32.exe veranschaulicht wird

**Wichtig:** Ein SID ist eine eindeutige Nummer, die Benutzer-, Gruppen- und Computerkonten identifiziert. Diese ist einmalig im Netz und darf nicht doppelt vorkommen. Falls für die Installation eine Antwortdatei auf Diskette erstellt wird, muss diese von **Unattend.txt** in **Winnt.sif** umbenannt werden, da sonst die unbeaufsichtigte Installation von Windows 2000 nicht funktionieren würde.

### Verwenden der Festplattenduplizierung

- Untersuchen des Vorgangs zur Festplattenduplizierung
- Verwenden des Systemvorbereitungsprogramms SYSPREP.EXE

<u>Wichtigste Vorraussetzung:</u> die Computer sollten Hardwaremäßig nahezu identisch sein

#### Untersuchen des Vorgangs zur Festplattenduplizierung

Der Vorgang zur Festplattenduplizierung besteht aus folgenden Aufgaben:

- 1. Windows 2000 auf einem Testcomputer installieren
- 2. alle benötigten Anwendungen auf dem Computer installieren
- 3. auf dem Testcomputer **SYSPREP.EXE** ausführen (anschließend werden **Computername, SID** und alle eindeutigen Konfigurationsvariablen vom Testcomputer entfernt, damit es später keine Probleme gibt)
- 4. Testcomputer neu starten und die **Software eines Drittanbieters** (z.B. Ghost oder Drive Image) ausführen, um ein Image der Festplatte zu erstellen
- 5. das Image auf einem freigegebenen Ordner oder auf CD speichern.
- 6. das Image auf mehrere Zielcomputer kopieren
- 7. Zielcomputer starten und den Installationsvorgang beenden

Wenn der Zielcomputer gestartet wird, fordert das "Mini-Installationsprogramm" die Benutzer auf, computerspezifische Variablen (z.B. Administratorkennwort, Computernamen...) einzugeben.

Alternativ kann statt **SYSPREP.EXE** auch der Assistent für den Installationsmanager gestartet werden, um einen anderen Typ von Antwortdatei namens **sysprep.inf** zu erstellen. **Sysprep.inf** stellt Antworten für ein "Mini-Installationsprogramm" bereit, das auf den Zielcomputern ausgeführt wird. Mit dieser Datei können außerdem benutzerdefinierte Treiber angegeben werden. Bei der Verwendung dieser .INF Datei wird beim Start des Zielcomputers Windows 2000 **ohne Benutzereingriff** installiert.

## Verwenden des Systemvorbereitungsprogramms SYSPREP.EXE

Sysprep.exe bereitet die Festplatte des Mastercomputers auf die Duplizierung vor. Eine der Hauptfunktionen ist das **Löschen von SID's** und allen anderen **benutzer**oder **computerspezifischen Informationen**. Windows 2000 erzeugt neue SID's, wenn die Zielcomputer nach dem Laden des Festplattenabbildes neu gestartet werden.

Folgende Schalter können mit Sysprep.exe verwendet werden:

Schalter	Aufgabe
-quiet	Ermöglicht die Ausführung ohne Benutzereingriff
-pnp	Zwingt das Installationsprogramm zur Erkennung von Plug & Play Geräten auf dem Zielcomputer
-reboot	Startet den Testcomputer neu
-nosidgen	Verhindert das erneute Erstellen von SID`s auf den Zielcomputern

# <u>Installieren von Windows 2000 mit Hilfe von RIS (Remote Installation Services)</u>

- Installieren und Konfigurieren der Remoteinstallationsdienste
- Konfigurieren von Clients für die Remoteinstallation

Vor dem Installieren von RIS müssen folgende Netzwerkdienste verfügbar sein:

- DNS-Server
- DHCP-Server
- Active-Directory
- RIS-Server

## Konfigurieren von Clients für die Remoteinstallation

Mindestens <u>eine</u> der folgenden Spezifikationen muss der Client erfüllen, um eine Remoteinstallation durchführen zu können:

- eine Konfiguration, die der **Net-PC** Spezifikation entspricht
- einen Netzwerkadapter mit **PXE-Boot-ROM** (für die Verbindung zum Server)
- einen unterstützten Netzwerkadapter und eine Startdiskette für die Remoteinstallation

Wichtig: RIS unterstützt zur Zeit noch keine tragbaren Computer.

# Unterrichtseinheit 16

### Implementieren von Windows 2000 basierten Servern

### Verfügbare Serverfunktionen:

- Dateiserver
- Druckserver
- Webserver: bei W2Kpro (Personal Web Server), bei W2Kserver (IIS)
- Anwendungsserver: z.B. Datei- und Druckserver, SQL-Server
- Domänencontroller: für Active Directory
- DNS-Server: setzt Domänennamen in IP-Adressen um
- WINS-Server: setzt NetBios Computernamen in IP-Adressen um (WinNT4.0)
- DHCP Server

#### Lastenausgleich

In einer großen Netzwerkumgebung ist ein Server für einen bestimmten Zweck dediziert. Die meisten Server erfüllen eine bestimmte Funktion (z.B. DHCP), oder fungieren als Domänencontroller, Datei-, oder Druckserver.

In kleineren Netzwerken hingegen erfüllt ein Server mehrere Funktionen gleichzeitig. In so einem Fall müssen die Funktionen gleichmäßig verteilt werden, um den Server nicht zu überlasten. Eine Möglichkeit besteht darin, die von Servern ausgeführte Funktionen in Tasks aufzuteilen, welche sich auf die allgemeinen Kategorien von Subsystemen auswirken: Arbeitsspeicher, Prozessor, Festplatte und Netzwerk. Jeder Task hat zwar Auswirkungen auf jedes Subsystem, jedoch trifft dies auf bestimmte Bereiche besonders zu.

#### Standardmäßige Serverfunktion

#### Primär betroffenes Subsystem

Domänencontroller Dateiserver Druckserver Anwendungsserver Webserver DNS- Server	Prozessor, Netzwerk Arbeitsspeicher, Festplatte Arbeitsspeicher, Prozessor Prozessor, Arbeitsspeicher Arbeitsspeicher, Festplatte Prozessor, Netzwerk	
DHCP – Server	Prozessor, Netzwerk	

### Dokumentieren der Supporttätigkeiten

Um die Probleme in einem Netzwerk möglichst gering zu halten, ist eine gute Dokumentation unvermeidlich. Dazu gehören unter anderem:

- ✓ Installationsdokumentation
- ✓ Konfigurationsinformationen
- ✓ Kontoänderungen
- ✓ Systemfehler des Servers und korrigierende Aktionen
- ✓ Sicherheitsverletzungen und Beschädigung durch Viren
- ✓ Service Packs, Aktualisierungen und Installationen
- ✓ Hardwareausfälle

### Allgemeine Implementierungsschritte

- installieren eines Betriebssystems
- beitreten einer Domäne oder Arbeitsgruppe
- vorbereiten von Laufwerken
- einrichten einer Datenstruktur
- einrichten von NTFS- und Freigabeberechtigungen
- testen und überprüfen des Systems

### Implementieren eines Dateiservers

- vorbereiten der Festplatten für den Dateiserver
- einrichten einer Datenstruktur
- einrichten von NTFS- Berechtigungen und von Berechtigungen für freigegebene Ordner
- verwenden von Dateiservern

Für einen Dateiserver ist es äußerst wichtig, dass Schutz für Dateien, genügend Speicherplatz und die Möglichkeit zum Wiederherstellen von Dateien bei einem Festplattenausfall bereitgestellt wird. Um dies zu gewährleisten ist folgende Festplattenkonfiguration auf Dateiservern häufig anzutreffen:

Die System – und Startpartition wird als gespiegelter oder RAID5 Datenträger eingerichtet.

Die **verbleibenden Datenträger** werden **als RAID5** Stripesetdatenträger für effiziente Verwendung von Festplattenspeicher angelegt.

Ein Dateiserver kann für folgende Zwecke genutzt werden:

- um Anwendungen für ältere Clientcomputer mit begrenzter Speicherkapazität zu speichern
- um die mehrfache Installation von Anwendungen auf mehreren Clients zu minimieren
- um zentralen Zugriff auf Anwendungen zu ermöglichen (als ein Verteilungsserver für Clientanwendungen, oder um Programme auf CD für den zentralen Zugriff zu speichern)

### Vorbereiten der Festplatten für Druckserver

Druckserver müssen zum Verwalten von Druckaufträgen über genügend **Festplattenspeicher** und **RAM** verfügen. Im Idealfall verfügt ein Druckserver über mindestens zwei Festplatten (eine für das **Betriebssystem**, die **Startdateien** und die **Auslagerungsdatei** und eine für den **SPOOLORDNER**).

Dabei sollte die **System- und Startpartition gespiegelt** werden, um Ausfallzeiten möglichst gering zu halten.

## Konfigurieren von Druckerfreigaben und -rechten

Nach der Installation und Freigabe eines Druckers muss der Administrator entscheiden, welche Benutzer diesen verwenden dürfen und wer für die Wartung des Druckers zuständig sein soll. Es müssen folgende Aspekte bedacht werden:

- welche Gruppen benötigen Zugriff auf den Drucker?
- soll die Verwaltung des Druckers einem Benutzer zugewiesen werden?
- muss Aufgrund eines erhöhten Druckaufkommens ein Druckerpool eingerichtet werden?
- Welche(r) Gruppe/Benutzer darf mit welcher Priorität drucken?
- soll Internetdrucken und Active Directory verwendet werden, um den Benutzern der Druckerzugriff zu vereinfachen?

## Vorbereiten der Festplatten für einen Anwendungsserver

Das Konfigurieren des Anwendungsservers ähnelt sehr dem des Dateiservers. Datenschutz und Fehlertoleranz ist hier sehr wichtig, so dass die Konfiguration der Festplatten identisch zu der des Dateiservers ist. Die einzige Ausnahme ist die Sicherung der Dateien. Während bei einem Dateiserver eine Sicherung pro Tag ausreicht, müssen beim Anwendungsserver mehrere Sicherungen pro Tag durchgeführt werden, um den reibungslosen Datenaustausch zu gewährleisten.

Da die meisten Client/Server Anwendungen auch für Mehrprozessorsysteme programmiert werden, ist es empfehlenswert, einen Anwendungsserver dementsprechend mit mehreren Prozessoren auszustatten.