Windows Vista

Christian Zahler

Drucker

Man unterscheidet grundsätzlich:

- **Physischer Drucker**
- **Logisches Druckerobjekt**

Unter einem **physischen Drucker** versteht man die eigentliche Hardware. Einem **physischen Drucker** können mehrere logische Druckerobjekte (mit unterschiedlichen Treibern und Konfigurationseinstellungen) zugeordnet werden; umgekehrt kann ein logisches Druckerobjekt mit mehreren physischen Druckern gleicher Bauart verknüpft werden („Druckerpool").

Unter einem **logischen Druckobjekt** versteht man die Kombination eines Druckertreibers (Software) mit bestimmten Konfigurationseinstellungen. Um also von Windows aus drucken zu können, muss ein **logisches Druckerobjekt** eingerichtet werden. Dabei unterscheidet man grundsätzlich:

- **Lokale Drucker(objekte)**
- **Netzwerkdrucker(objekte)**

Lokale Druckerobjekte werden lokal erstellt. Sie werden in der lokalen Registrierdatenbank (Registry) des jeweiligen Rechners gespeichert.

Lokale Druckerobjekte müssen mit einem Treiber und Anschlussinformationen hinterlegt werden.

Es ist nicht zwingend nötig, dass der Drucker physisch mit dem PC verbunden ist; so gelten auch Drucker mit eingebauter oder externer Netzwerkkarte (umgangssprachlich auch als „Printserver" bezeichnet) als lokale Drucker.

Arten von Anschlüssen:

- Parallel (LPT1)
- Seriell (COM1)
- USB
- Netzwerkkarten mit IP-Adresse

Netzwerkdruckerobjekte verweisen zu freigegebenen lokalen Druckerobjekten, die auf einem anderen PC erstellt wurden.

Netzwerkdruckerobjekte müssen mit einem UNC-Pfad zur entsprechenden Freigabe hinterlegt werden, zum Beispiel `\\server02\HPLaserJet`.

Ablauf des Druckvorgangs

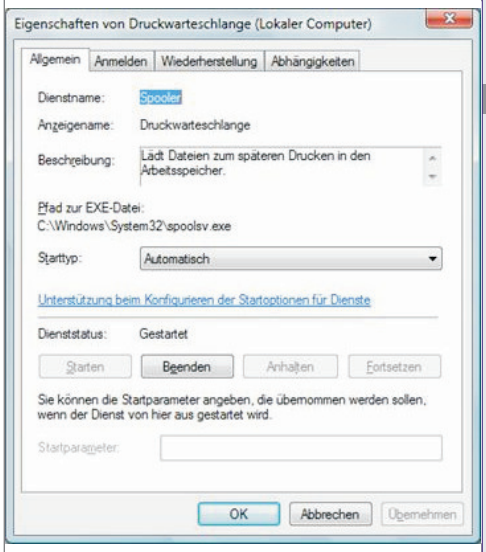
Wird ein Druckvorgang durchgeführt, so laufen dabei folgende Schritte ab:

1. Je nach installiertem Drucker wird eine Druckdatei erstellt. Diese Druckdatei kann zum Beispiel in den Druckersprachen PCL *(Printer Control Language)*, PS *(PostScript)* oder HOPGL *(Hewlett Packard Graphics Language)* geschrieben sein. Es handelt sich dabei immer um eine Textdatei, die Anweisungen an den jeweiligen Drucker enthält.

Ausschnitt einer PostScript-Druckdatei:

```
F /F0 0 /256 T /Helvetica mF
/F0S53 F0 [83 0 0 -83 0 0 ] mFS
F0S53 Ji
473 550 M (Dieser Text soll gedruckt
werden.)[60 18 46 42 46 28 23 52 46 42 23 23 42
46 18 18 24 46 46 46 29 46 42 43 23 23 59 46 28
46 46 46
 0]xS
1708 550 M ( )S
473 646 M ( )S
LH
(%%[Page: 1]%%) =
%%PageTrailer
```

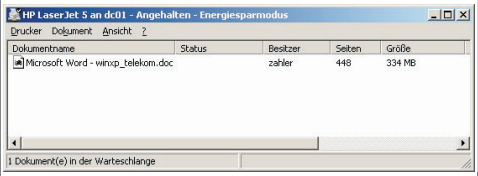
2. Diese Druckdatei wird an den **Druckspooler** *(Spool = Simultaneous Peripheral Operation On-Line)* weitergeleitet. Es handelt sich dabei um einen lokal operierenden Dienst, der Druckaufträge (englisch: Jobs) in Druckwarteschlangen (englisch: Queues) verwaltet.



Die Druckwarteschlangen können lokal vorhanden sein – oder, im Fall eines Druckservers – auch auf anderen Rechnern.

Wichtig: Für die Druckaufträge muss ausreichend Platz auf der Festplatte vorhanden sein (Druckaufträge können mehrere 100 MB groß werden, siehe Abbildung!).

In der Druckwarteschlangenverwaltung können Druckaufträge gelöscht werden, der Drucker „angehalten" werden (das bedeutet, der Spool-Vorgang wird unterbrochen).



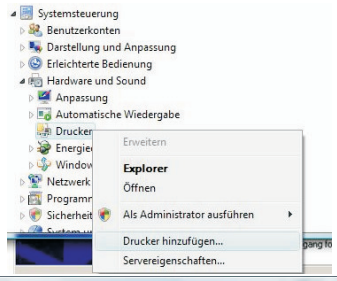
3. Die Druckdateien werden dann an den angegebenen Drucker weitergeleitet. Dabei kann der Drucker immer nur so viele Daten empfangen, wie er in seinem Arbeitsspeicher unterbringen kann.

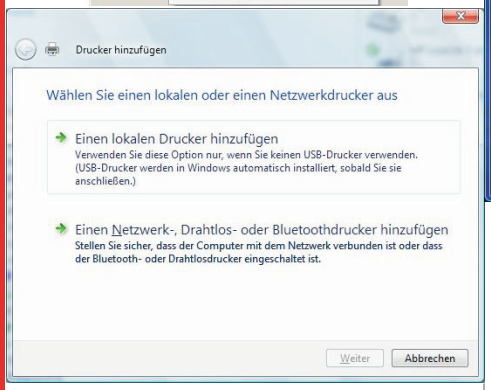
4. Der Drucker arbeitet die in seinem Arbeitsspeicher befindlichen Druckaufträge seitenweise (Laserdrucker) bzw. zeilenweise (Nadel-, Tintenstrahldrucker) ab. Nicht benötigte Druckinformationen werden gelöscht, sodass im RAM Platz für weitere Teile des Druckauftrags bzw. neue Druckaufträge geschaffen wird.

Inhaltsverzeichnis

Einrichten eines lokalen Druckerobjekts

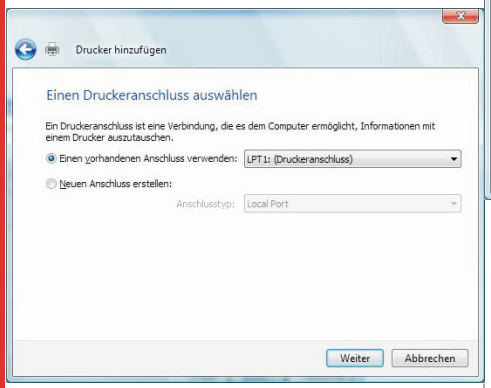
Über die Systemsteuerung im Objekt *„Drucker und Faxgeräte“* auf *„Drucker hinzufügen“* klicken. Es startet folgender Assistent:





1. Schritt: Geben Sie im Assistenten an, dass ein lokales Druckerobjekt erstellt werden soll. Wenn der Drucker tatsächlich physisch an den PC **angeschlossen und eingeschaltet** (!) ist, kann das Kontrollkästchen *„Plug & Play-Drucker automatisch ermitteln und installieren“* aktiviert bleiben.

2. Schritt: Wählen Sie den **Druckeranschluss** aus oder erstellen Sie einen neuen Anschluss.

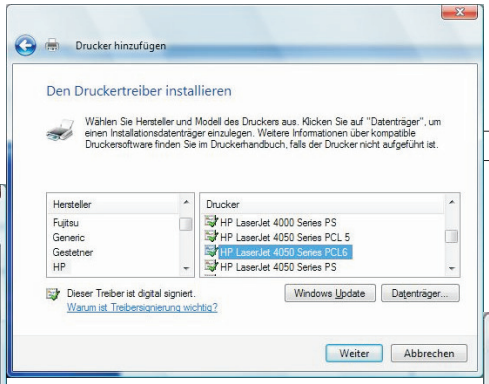


Folgende Anschlüsse sind bereits standardmäßig vorhanden:

- **Parallele Anschlüsse (LPT1, ...)**: Früher der Standard-Druckeranschluss; erforderlich ist ein paralleles Kabel mit Centronics-Stecker.
- **Serielle Anschlüsse (COM1, ...)**: Wurde häufig für CAD-Plotter verwendet. Voraussetzung für das Funktionieren des Druckers ist die übereinstimmende Konfiguration der seriellen Schnittstellen auf PC und Drucker (zum Beispiel Übertragungsrate – 9600 bps).
- **Umleitung in Datei (FILE:):** Die Druckdaten werden nicht an den Druckspooler gesendet, sondern in eine Druckdatei geschrieben (Dateierweiterung *.prn). Der Ausdruck selbst kann dann später bzw. auf einem nicht lokal vorhandenen Drucker erfolgen.
- **Microsoft Document Imaging Writer Port (Local Port):** Ist Office 2003 auf dem PC installiert, so kann mit diesem Anschluss eine `*.mdi`-Datei erzeugt werden, ein sehr platzsparendes Format, das nicht mehr bearbeitet werden kann, aber mit dem Microsoft Document Imaging-Tool betrachtet und gedruckt werden kann (ähnlich PDF).

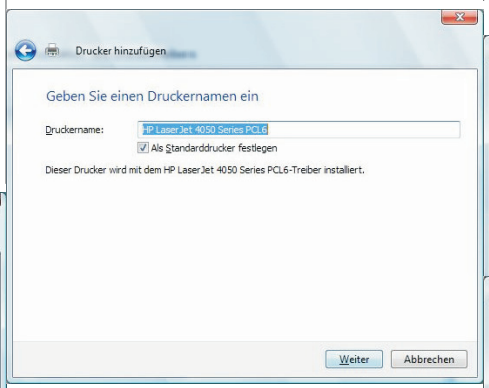
Nicht vorhanden sind TCP/IP-Anschlüsse, die gebraucht werden, wenn der Drucker über eine Netzwerkkarte verfügt, die mit dem Netzwerk verbunden ist (siehe später).

3. Schritt: Auswählen des **Druckertreibers**



4. Schritt: Drucker benennen, Standarddrucker konfigurieren

Die Konfiguration als Standarddrucker ist insofern wesentlich, als viele Softwaretools grundsätzlich auf dem Standarddrucker auswählen (zum Beispiel wird bei der Druckerauswahl im Menü *[Datei] – [Drucken]* nur der Standarddrucker geändert!).



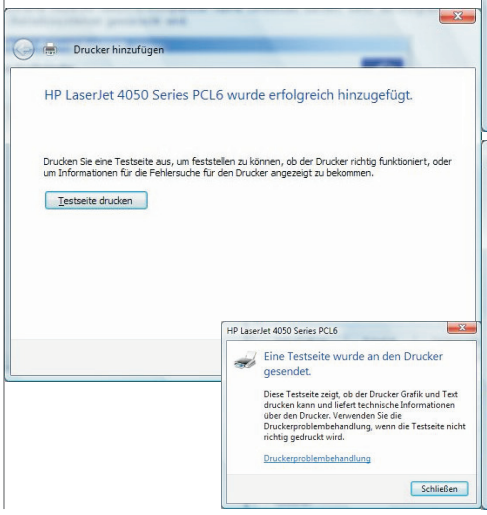
Nun werden die nötigen Treiber installiert.

5. Schritt: Testseite drucken

Eine letzte Kontrolle des eingerichteten Druckers stellt die Testseite dar, die aus

- grafischen Informationen,
- Systemschrift-Texten und
- TrueType-Schrift-Texten

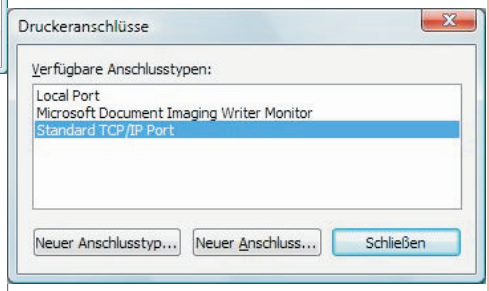
besteht. Überprüfen Sie speziell, ob diese drei Elemente korrekt dargestellt werden. Wenn nicht, sollten Sie einen anderen Druckertreiber wählen.



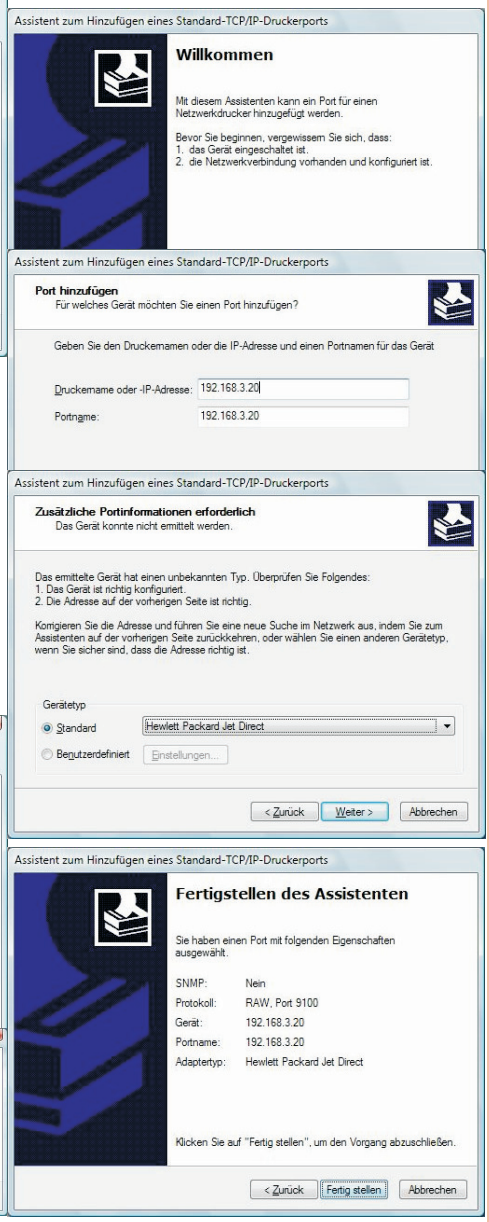
So sollte eine Drucker-Testseite aussehen:

Erzeugen eines TCP/IP-Druckeranschlusses

Dies ist notwendig, wenn der lokale Drucker über eine eigene Netzwerkkarte bzw. über eine externe Netzwerkkarte (falsch auch als „Printserver“ bezeichnet, etwas korrekter „Netport“) verfügt.



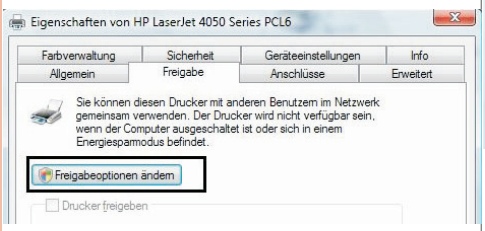
Druckserver konfigurieren:



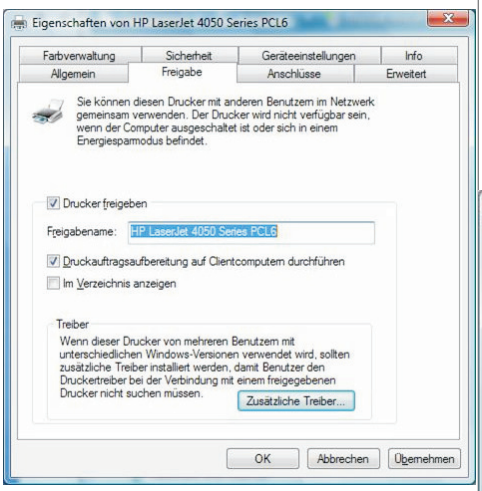
Schritt 1: Drucker freigeben

Eine Druckerfreigabe basiert auf denselben technischen Grundlagen wie Ordnerfreigaben. Als Freigabename muss ein NetBIOS-kompatibler Name verwendet werden, wenn die Integration mit älteren Betriebssystemen gewünscht wird.

Zunächst müssen die Freigabeoptionen des logischen Druckerobjekts geändert werden:



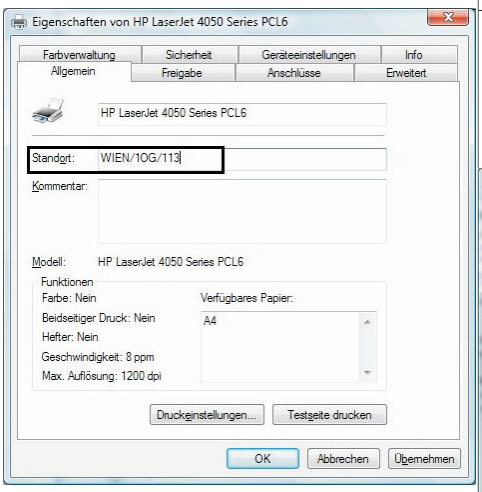
Dann muss ein Freigabename festgelegt werden:



Wichtig: Ein freigegebener Drucker wird auch als Druck-Server bezeichnet!

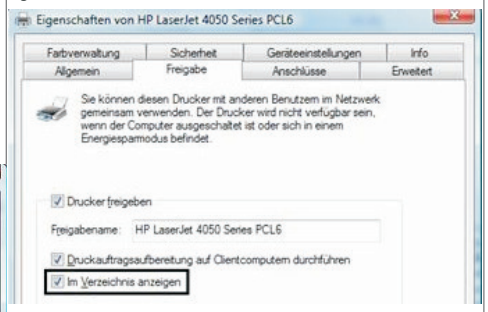
2. Schritt: Standortangabe und Kommentar

Bei der Angabe des Standorts sollten Sie eine Hierarchie berücksichtigen, mit Hilfe derer der Drucker wieder gefunden werden kann.

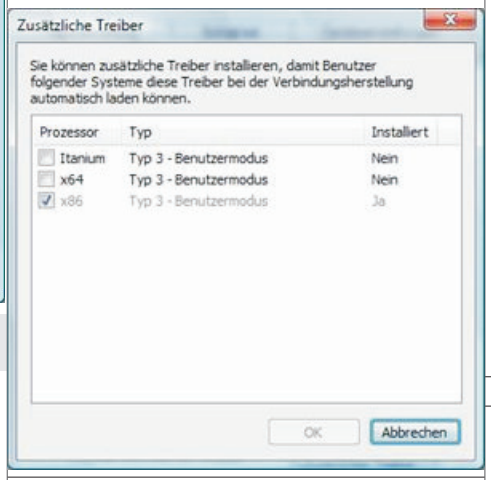


Wenn Sie einen Druckserver konfiguriert haben (zur Erinnerung: das ist ein freigegebener Drucker), dann haben Sie zwei weitere Möglichkeiten:

- Veröffentlichung der Druckerfreigabe im Active Directory (nur in AD-Domänen möglich): Dazu muss der Eintrag *„Im Verzeichnis anzeigen"* aktiviert werden

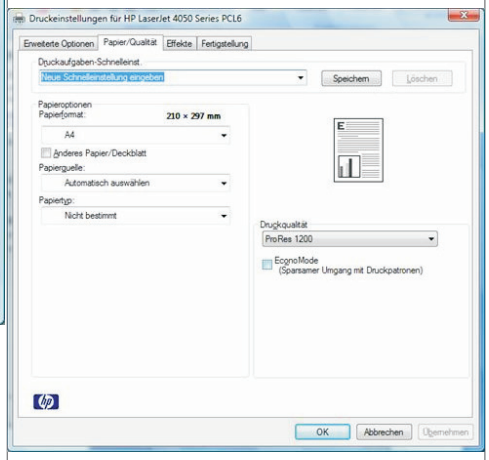


- Bei der Freigabe von Druckern wird automatisch eine administrative Freigabe **PRINT$** erzeugt, die zu einem Ordner führt, in welchem passende Druckertreiber vorhanden sind. Bei der Installation eines Netzwerkdruckers können Client-PCs diese Treiber herunterladen, ohne das Druckermodell kennen zu müssen. Standardmäßig werden in diese Freigabe nur Treiber für Windows 2000/XP/2003 gestellt; mit der Schaltfläche *„Zusätzliche Treiber"* können auch Treiber für ältere Windows-Plattformen in diese Freigabe gestellt werden.

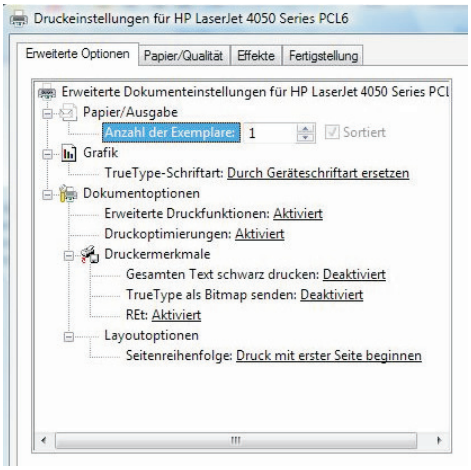


Druckeinstellungen

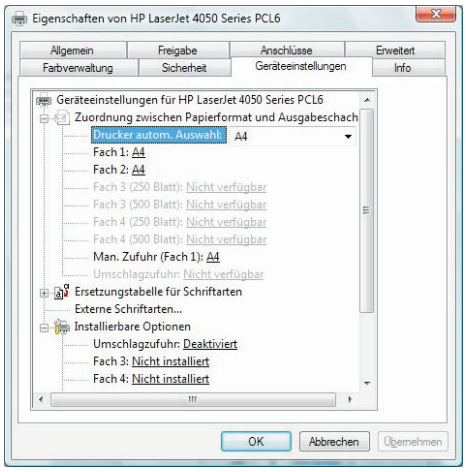
In den Eigenschaften jedes logischen Druckerobjekts können Druckeinstellungen konfiguriert werden. Typische Einstellungen betreffen das Papierformat oder die Reihenfolge, in welcher Seiten ausgedruckt werden sollen.



Unter *„Erweitert"* lassen sich noch weitere Parameter – abhängig vom verwendeten Druckermodell – konfigurieren.



Die Karteikarte *„Geräteeinstellungen"* enthält Konfigurationseinstellungen zu Papierschächten, Postscript-Optionen und Drucker-RAM.

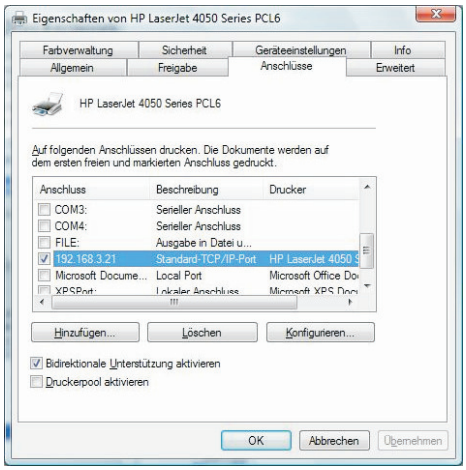


Einrichten eines Druckerpools

Unter einem Druckerpool versteht man mehrere gleichartige physische Drucker, die unter demselben Namen im Netzwerk angesprochen werden sollen. Es ist daher **ein** logisches Druckerobjekt zu erstellen, welchem **zwei** oder mehrere physische Drucker zugeordnet werden.

Dazu ist es nötig, zuerst einen der beiden Drucker wie beschrieben zu installieren und dann die Eigenschaften des logischen Druckerobjekts zu bearbeiten.

Zunächst muss ein zweiter Druckeranschluss hinzugefügt werden (da es sich in der Praxis meist um TCP/IP-Drucker handelt, sind in der Abbildung zwei TCP/IP-Ports dargestellt):

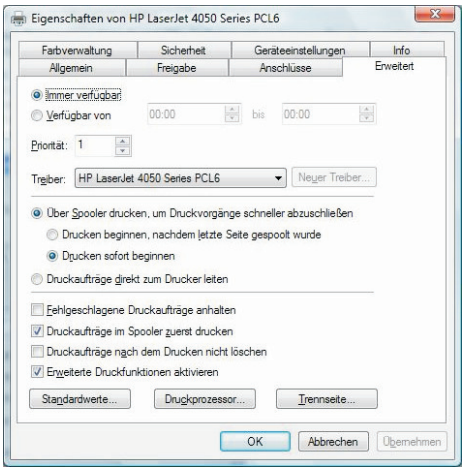


Danach muss die Einstellung *„Druckerpool aktivieren"* angekreuzt werden; beachten Sie, dass alle Anschlüsse, die zum Druckerpool gehören sollen, mit Kontrollkästchen aktiviert sein müssen!

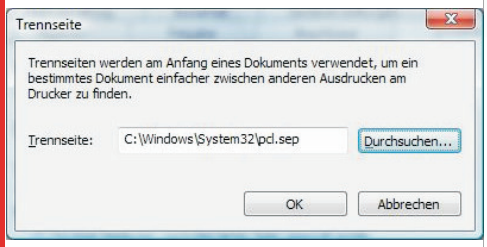
Erweiterte Druckereigenschaften

In der Karteikarte *„Erweitert"* kann konfiguriert werden:

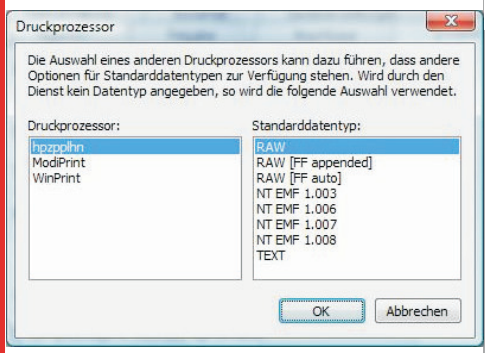
- **Priorität der Druckaufträge** (zwischen 1 und 99): Aufträge mit geringerer Priorität werden in der Druckwarteschlage nachgereiht und daher später gedruckt.
- **Spooler umgehen**: Hier kann der Druckauftrag direkt zum Drucker gesendet werden. Das hat den Nachteil, dass der Druckvorgang länger dauert, da der im Drucker vorhandene RAM meist zu klein ist, um den kompletten Druckauftrag zwischenzuspeichern. Deshalb muss gewartet werden, bis der komplette Druckauftrag zum Drucker gesendet wurde, bevor weitergearbeitet werden kann.



- **Trennseite**: Hier ist es möglich, eine Trennseite für Druckaufträge zu konfigurieren, auf der Informationen wie der Benutzername des Auftraggebers enthalten sind.



- **Druckprozessor**: Hier kann die Verarbeitung von Grafiken geändert werden. Die voreingestellte Konfiguration *(WinPrint / RAW)* ist für viele Anwendungen ideal und muss nicht angepasst werden.



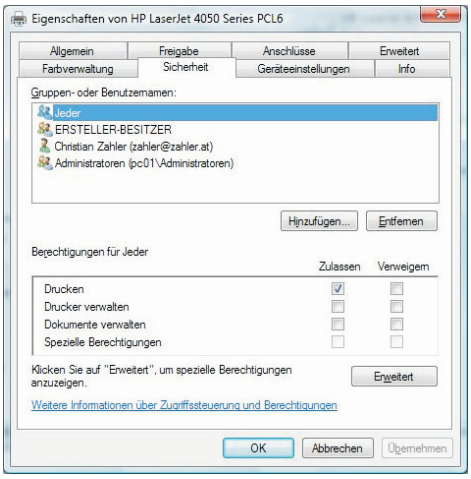
NTFS-Berechtigungen für logische Druckerobjekte

So wie für Dateien und Ordner können auch NTFS-Berechtigungen für logische Druckerobjekte erstellt werden.

Für Drucker existieren spezielle Berechtigungen:

- Drucken (das muss nicht speziell erklärt werden)
- Dokumente verwalten (mit dieser Berechtigung können Druckaufträge aus der Druckwarteschlange entfernt werden)
- Drucker verwalten (damit können logische Druckerobjekte umkonfiguriert werden)

Standardmäßig hat nur die Spezial-Identität `ERSTELLER-BESITZER` das Recht, Druckaufträge zu löschen. Das hat zur Folge, dass ein normaler Benutzer nur seine eigenen Druckaufträge aus der Warteschlange löschen kann, solange er nicht eine andere NTFS-Berechtigung bekommen hat.



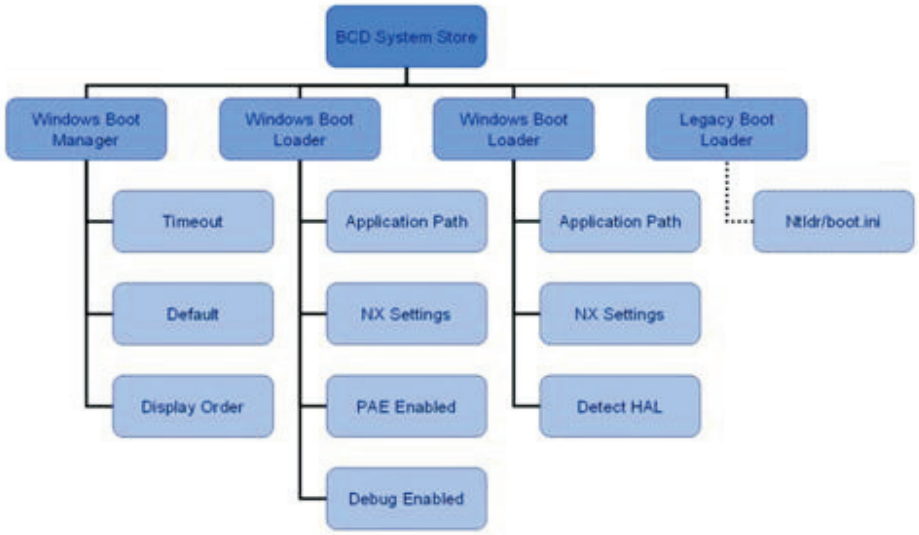
Startvorgang, Datenträgerverwaltung und Notfallwiederherstellung

Startvorgang von Windows Vista

Die wichtigsten Komponenten während des Startvorgangs von Windows Vista findet man im Stammverzeichnis der Startpartition:

- **bootmgr**: Diese Applikation kontrolliert den Windows Vista Startvorgang. In einer Multiboot-Umgebung stellt bootmgr das Betriebssystem-Auswahlmenü dar. Bis Windows XP/Server 2003 war das Programm ntldr für diese Aufgaben verantwortlich.
- **Boot Configuration Data (BCD)**: Windows Vista speichert Startkonfigurationen in BCD. Das Programm `bootmgr` liest BCD, um das Betriebssystem-Auswahlmenü darstellen zu können. BDC ist der Nachfolger der Datei `boot.ini`, die in früheren Windows-Versionen verwendet wurde. Die Datenstruktur im BCD ist ähnlich wie ein Registry-Hauptschlüssel gespeichert und kann nicht direkt mit einem Texteditor bearbeitet werden.

Beispiel (Quelle: *www.tecchannel.de*): Der BCD-Store enthält ein Objekt für den Bootmanager, zwei für Vista/Windows Server 2008 und einen für Windows XP/2000/2003.

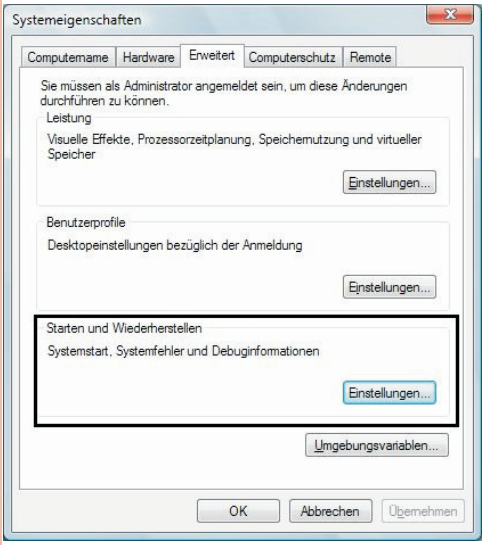


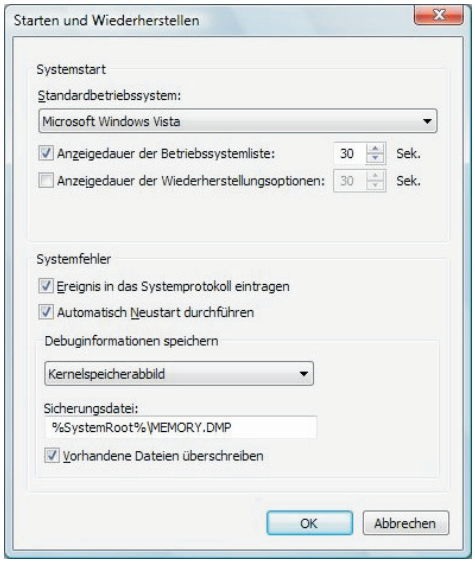
- `Winload.exe`: Dieses Programm lädt das Betriebssystem selbst. Fall aus dem Betriebssystem-Auswahlmenü Windows Vista ausgewählt wird, so wird die Kontrolle an `Winload.exe` übergeben. Es lädt den Kernel, das *Hardware Abstraction Layer* (HAL) und diverse Treiber in den Arbeitsspeicher. In einer Multiboot-Umgebung hat jede Windows Vista-Instanz ihren eigenen winload.exe.
- `Winresume.exe`: Das ist das *„Wiederaufnahme-Startprogramm"* für Windows Vista, falls das Betriebssystem aus dem Energiesparmodus wieder *(engl. „hibernation mode")* in Betrieb genommen wird.

In früheren Windows-Versionen konnte die Datei `boot.ini` manuell mit jedem beliebigen Text-Editor verändert werden.

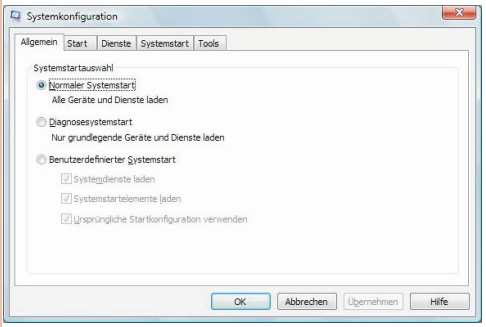
Der Startvorgang kann mit folgenden Methoden verändert werden:

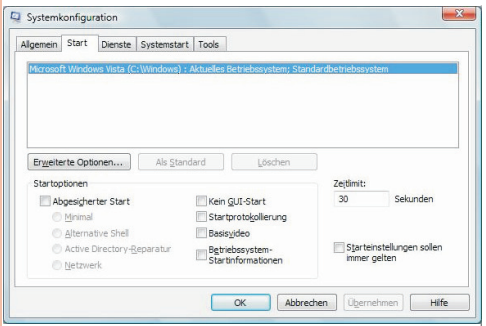
- ***Systemeigenschaften***, Karteikarte ***„Erweitert"***, Rubrik ***„Start und Wiederherstellung"***:





- Systemkonfiguration (`msconfig.exe`)





- **`BCDEdit`**: Dieses Tool ermöglicht die umfangreichsten Konfigurationsmöglichkeiten („fast alle") für den Startvorgang. Damit ist auch ein Export und Import von Konfigurationsdaten möglich.

Beispiel: Anzeige aktueller Konfigurationsdaten:

```
C:\>bcdedit /enum

Windows-Start-Manager
---------------------
Bezeichner              {bootmgr}
device                  partition=C:
description             Windows Boot Manager
locale                  de-DE
inherit                 {globalsettings}
default                 {current}
resumeobject
{a7cf2159-9ce5-11db-9b34-824fb58ca61f}
displayorder            {current}
toolsdisplayorder       {memdiag}
timeout                 30

Windows-Startladeprogramm
-------------------------
Bezeichner              {current}
device                  partition=C:
path
\Windows\system32\winload.exe
description             Microsoft Windows Vista
locale                  de-DE
inherit                 {bootloadersettings}
osdevice                partition=C:
systemroot              \Windows
resumeobject
{a7cf2159-9ce5-11db-9b34-824fb58ca61f}
nx                      OptIn
```

- **Windows Management Interface (WMI)**: Diese Programmierschnittstelle ist die einzige Möglichkeit, kompletten Zugriff auf den BCD-Speicherbereich zu bekommen.

Backup und Restore, Notfallwiederherstellung

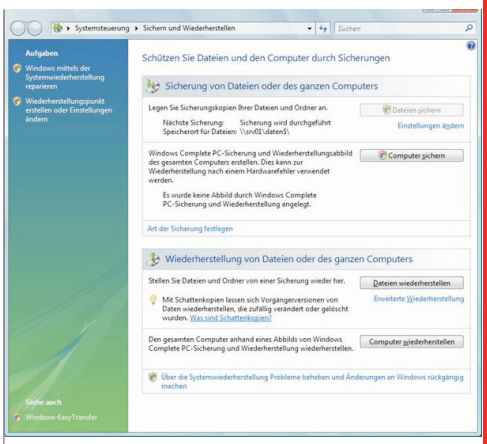
Backup

Windows Vista unterstützt Sie bei der Sicherung von PC-Einstellungen, Dateien und Anwendungen zum gewünschten Zeitpunkt und am gewünschten Speicherort und bietet eine automatische Zeitplanung. Windows Vista bietet eine umfassendere und auch benutzerfreundlichere Sicherungsumgebung als das einfache Sicherungsprogramm unter Windows XP. Das neue Feature ***"Sicherung"*** bietet mehr Optionen für das Speichern Ihrer gesicherten Informationen. Sie können Daten auf CD-ROM, DVD-ROM, einer externen Festplatte, die über USB oder IEEE 1394 am PC angeschlossen ist, einer anderen Festplatte im PC oder einem anderen mit dem Netzwerk verbundenen PC oder Server sichern.

Unter Windows Vista ist der Sicherungsvorgang auch einfacher als unter Windows XP. Sie müssen Datensicherungen nicht mehr manuell durchführen, da es jetzt einen einfachen Assistenten gibt, mit dem Zeitpunkt und Speicherort von Sicherungen geplant werden können.

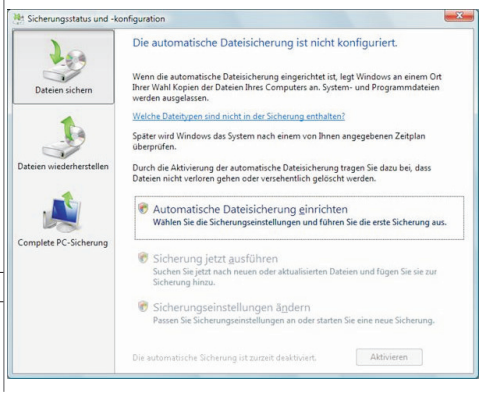
Eine Sicherungsumgebung ist freilich nur so nützlich wie die dazugehörige Wiederherstellungsumgebung, deren Umfang und Nutzen unter Windows Vista erweitert wurde. Ein Assistent hilft bei der Auswahl der wiederherzustellenden Dateien und Ordner und fordert die Angabe von Wiederherstellungsmedien an. Anschließend werden die ausgewählten Dateien wiederhergestellt.

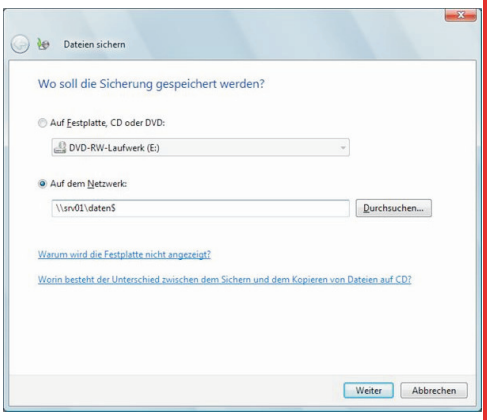
In der Systemsteuerung werden unter der Rubrik ***„Sichern und Wiederherstellen"*** grundsätzlich zwei Methoden vorgeschlagen:

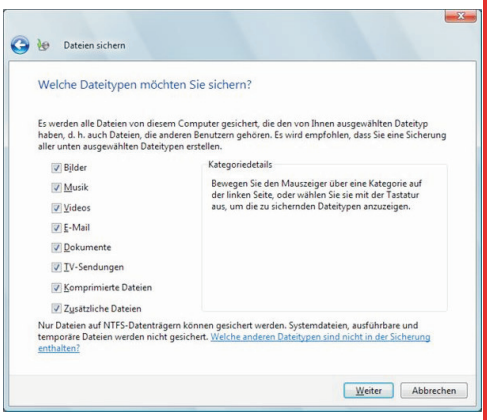


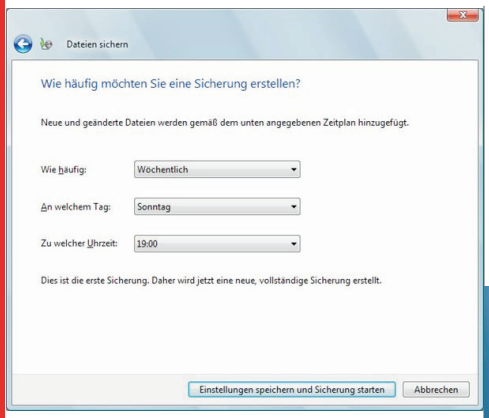
- Sicherung einzelner Dateien
- Sicherung des gesamten Computers

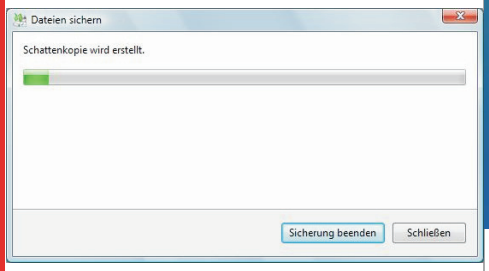
Die Sicherung einzelner Dateien erfolgt mit dem Assistenten ***„Sicherungsstatus und -konfiguration"***:

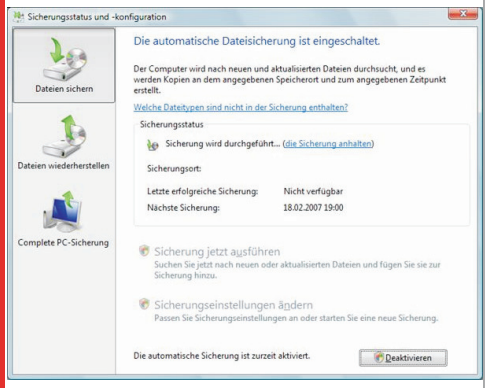




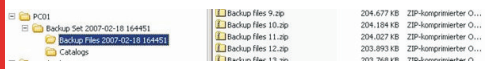






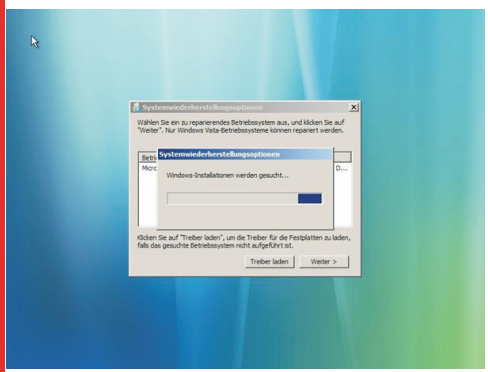


Aufbau des Backup-Verzeichnisses:



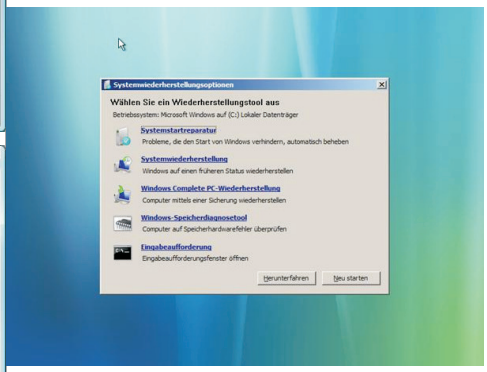
Startup Repair

Booten von DVD nötig, dann auf *„Reparieren"* klicken. Es werden dann die bestehenden Windows-Installationen gesucht:



Hier besteht über den Button *"Treiber"* auch die Möglichkeit, zusätzliche Treiber aus einer anderen Quelle zu laden. Nach der Auswahl der gewünschten Windows-Version wird ein neues Fenster geöffnet, welches die folgenden Möglichkeiten anbietet:

- **Systemreparatur**: Automatisches Reparieren von Windows Startproblemen (Bootsektor usw.)
- **Systemwiederherstellung**: Herstellen von Windows über vorhandene Wiederherstellungspunkte (Konfiguration von Wiederherstellungspunkten siehe nächstes Kapitel)
- **Windows komplette PC-Wiederherstellung**: Komplettes Wiederherstellen eines Windows-Backups
- **Windows-Speicherdiagnosetool**: Arbeitsspeicher auf Fehler überprüfen (Neustart erforderlich)
- **Eingabeaufforderung** (bis Windows XP/2003: *„Wiederherstellungskonsole"*): Kommandozeile/Eingabeaufforderung



In der Wiederherstellungskonsole stehen folgende Kommandos zur Verfügung:

Attrib ändert Attribute einer Datei oder eines Unterverzeichnisses.

Batch führt die in einer Textdatei angegebenen Befehle aus (Eingabedatei); Ausgabedatei enthält die Ausgabe der angegebenen Befehle. Wenn der Parameter Ausgabedatei nicht angegeben ist, wird die Ausgabe auf dem Bildschirm angezeigt.

Bootcfg dient zum Bearbeiten der Datei `Boot.ini` für die Startkonfiguration und die Wiederherstellung.

CD (Chdir) funktioniert nur innerhalb der Systemverzeichnisse der aktuellen Windows-Installation, auf Wechselmedien, im Stammverzeichnis einer Festplattenpartition oder in den lokalen Installationsverzeichnissen.

Chkdsk Der Parameter `/p` führt `Chkdsk` aus, auch wenn das Laufwerk als sauber markiert ist. Der Parameter `/r` sucht nach fehlerhaften Sektoren und stellt lesbare Daten wieder her; dieser Parameter impliziert `/p`. Chkdsk erfordert Autochk. Chkdsk sucht automatisch im Startverzeichnis nach `Autochk.exe`. Wenn Chkdsk die Datei nicht im Startverzeichnis finden kann, sucht Chkdsk nach der Windows-Installations-CD. Wenn Chkdsk die Installations-CD nicht finden kann, wird der Benutzer aufgefordert, den Pfad zur Datei `Autochk.exe` anzugeben.

Cls löscht den Bildschirminhalt.

Copy kopiert eine Datei in ein Zielverzeichnis. Das Ziel kann standardmäßig kein Wechselmedium sein, und es können keine Platzhalter verwendet werden. Beim Kopieren einer komprimierten Datei von der Windows-Installations-CD wird die Datei automatisch dekomprimiert.

Del (Delete) löscht eine Datei. Funktioniert nur innerhalb der Systemverzeichnisse der aktuellen Windows-Installation, auf Wechselmedien, im Stammverzeichnis einer Festplattenpartition oder in den lokalen Installationsverzeichnissen. Es können standardmäßig keine Platzhalter verwendet werden.

Dir zeigt eine Liste aller Dateien an, einschließlich versteckte und Systemdateien.

Disable deaktiviert einen Windows-Systemdienst oder -Treiber. Die Variable Dienst_oder_Treiber ist der Name des Dienstes oder Treibers, den Sie deaktivieren wollen. Wenn Sie diesen Befehl verwenden, um einen Dienst zu deaktivieren, wird der ursprüngliche Starttyp des Dienstes angezeigt, bevor der Typ in `SERVICE_DISABLED` geändert wird. Sie sollten sich den ursprünglichen Starttyp notieren, damit Sie den Befehl **Enable** verwenden können, um den Dienst wieder zu starten.

Diskpart verwaltet Partitionen auf Festplatten. Die Option `/add` erstellt eine neue Partition; die Option `/delete` löscht eine bestehende Partition. Die Variable Gerät ist der Gerätename für eine neue Partition (wie `\Gerät\Festplatte0`). Die Variable Laufwerk ist der Laufwerkbuchstabe für das Löschen einer bestehenden Partition (zum Beispiel `D`); Partition ist der Partitionsname für das Löschen einer bestehenden Partition (zum Beispiel `\Gerät\Festplatte0\Partition1`) und kann anstelle der Variable Laufwerk verwendet werden. Die Variable Größe ist die Größe einer neuen Partition in MB.

Enable aktiviert einen Windows-Systemdienst oder -Treiber. Die Variable `Dienst_oder_Treiber` ist der Name des Dienstes oder Treibers, den Sie aktivieren wollen, und `Starttyp` ist der Starttyp für einen aktivierten Dienst. Der Starttyp verwendet eines der folgenden Formate:

```
SERVICE_BOOT_START
SERVICE_SYSTEM_START
SERVICE_AUTO_START
SERVICE_DEMAND_START
```

Exit beendet die Wiederherstellungskonsole und startet den Computer neu.

Expand expandiert eine komprimierte Datei. Die Variable Quelle gibt die zu expandierende Datei an. Es können standardmäßig keine Platzhalter verwendet werden. Die Variable Ziel gibt das Verzeichnis für die neue Datei an. Das Verzeichnis kann standardmäßig kein Wechselmedium und kann nicht schreibgeschützt sein. Sie können den Befehl attrib verwenden, um den Schreibschutz des Zielverzeichnisses aufzuheben. Die Option `/f:filespec` ist erforderlich, wenn die Quelle mehr als eine Datei enthält; bei dieser Option können Platzhalter verwendet werden. Der Parameter `/y` deaktiviert die Bestätigungsaufforderung vor dem Überschreiben. Der Parameter `/d` gibt an, dass die Dateien nicht expandiert werden sollen und zeigt ein Verzeichnis der Dateien in der Quelle an.

Fixboot schreibt einen neuen Startsektor auf der Systempartition.

Fixmbr repariert den Master Boot Code der Startpartition. Die Variable Gerät ist ein optionaler Name, der das Gerät angibt, das einen neuen MBR benötigt; lassen Sie diese Variable weg, wenn das Ziel das Startgerät ist.

Format formatiert einen Datenträger. Der Parameter `/q` führt eine Schnellformatierung durch, der Parameter `/fs` gibt das Dateisystem an.

Help Wenn Sie nicht die Variable `Befehl` verwenden, um einen Befehl anzugeben, listet `help` alle Befehle auf, die die Wiederherstellungskonsole unterstützt.

Listsvc zeigt alle verfügbaren Dienste und Treiber auf dem Computer an.

Logon zeigt erkannte Windows-Installationen an und fordert die Eingabe des lokalen Administratorkennworts für diese Installationen. Verwenden Sie diesen Befehl, um zu einer an-

deren Installation oder einem anderen Unterverzeichnis zu wechseln.

Map zeigt die aktiven Gerätezuordnungen an. Fügen Sie die Option arc ein, um Advanced RISC Computing (ARC)-Pfade (das Format für `Boot.ini`) statt Windows-Gerätepfade zu verwenden.

MD (Mkdir) funktioniert nur innerhalb der Systemverzeichnisse der aktuellen Windows-Installation, auf Wechselmedien, im Stammverzeichnis einer Festplattenpartition oder in den lokalen Installationsverzeichnissen.

More/Type zeigt die angegebene Textdatei (z.B. den Dateinamen) auf dem Bildschirm an.

Rd (Rmdir) funktioniert nur innerhalb der Systemverzeichnisse der aktuellen Windows-Installation, auf Wechselmedien, im Stammverzeichnis einer Festplattenpartition oder in den lokalen Installationsverzeichnissen.

Ren (Rename) funktioniert nur innerhalb der Systemverzeichnisse der aktuellen Windows-Installation, auf Wechselmedien, im Stammverzeichnis einer Festplattenpartition oder in den lokalen Installationsverzeichnissen. Sie können kein neues Laufwerk/keinen neuen Pfad als Ziel angeben.

Set dient zur Anzeige und Definition der Umgebungsvariablen der Wiederherstellungskonsole.

Systemroot setzt das aktuelle Verzeichnis auf `%SystemRoot%`.

MRT Microsoft Tool zum Entfernen bösartiger Software. Dieses Tool überprüft, ob Trojaner auf Ihrem Rechner vorhanden sind.

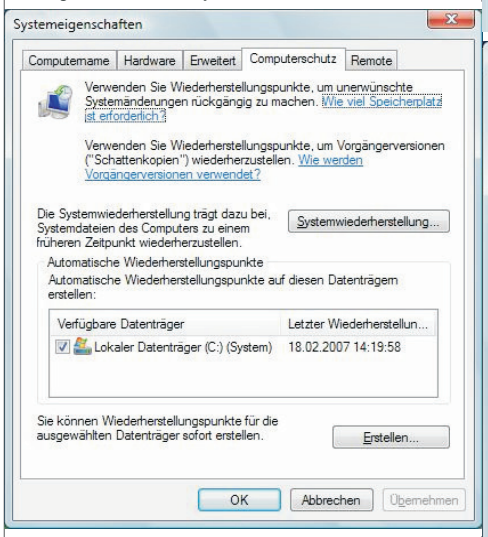
Systemwiederherstellung und Volumenschattenkopien („Volume Shadow Copies")

Die Systemwiederherstellung wurde unter Windows XP eingeführt, damit Benutzer ihre Computer in einen vorherigen Zustand zurückversetzen können, ohne persönliche Datendateien zu verlieren (wie z. B. Microsoft Office Word-Dokumente, Grafikdateien und E-Mail-Nachrichten). Für die Systemwiederherstellung müssen keine Systemsnapshots erstellt werden, da das System einfach erkennbare Wiederherstellungspunkte automatisch anlegt, mit deren Hilfe Sie Ihr System auf einen früheren Zeitpunkt zurücksetzen können. Wiederherstellungspunkte werden sowohl zum Zeitpunkt wichtiger Systemereignisse (z. B. bei der Installation von Anwendungen oder Treibern) als auch in regelmäßigen Abständen (täglich) erstellt. Sie können Wiederherstellungspunkte jederzeit erstellen und benennen.

Die Systemwiederherstellung unter Windows XP basiert auf einem Dateifilter, der Dateiänderungen für einen bestimmten Satz von Dateinamenerweiterungen überwacht und Dateien kopiert, bevor diese überschrieben werden. Wenn ein Problem auftritt, können Sie die Systemdateien und die Registrierung auf ein vorheriges Datum zurücksetzen, an dem das System bekanntermaßen ordnungsgemäß funktioniert hat.

Unter Windows Vista ermöglicht die Systemwiederherstellung eine Wiederherstellung nach einer größeren Vielfalt von Änderungen als unter Windows XP. Das Dateifiltersystem für die Systemwiederherstellung in früheren Versionen von Windows wurde durch eine neue Methode ersetzt. Wenn nun ein Wiederherstellungspunkt erforderlich ist, wird eine **Schattenkopie** einer Datei oder eines Ordners erstellt. Eine Schattenkopie ist im Wesentlichen eine frühere Version der Datei oder des Ordners zu einem bestimmten Zeitpunkt. Windows Vista kann Wiederherstellungspunkte automatisch oder nach Aufforderung erstellen. Wenn das System wiederhergestellt werden muss, werden Dateien und Einstellungen aus der Schattenkopie auf das aktive von Windows Vista verwendete Volume kopiert. Dadurch wird die Integration mit anderen Aspekten der Sicherung und Wiederherstellung verbessert und die Systemwiederherstellungsfunktion noch nützlicher.

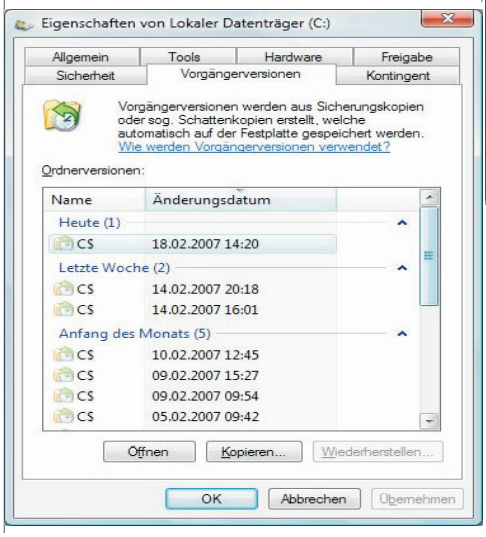
Aktivieren des Computerschutzes: Unter *Systemeigenschaften – Computerschutz*:



Schattenkopien werden automatisch als *Teil eines Wiederherstellungspunkts* in den Systemeigenschaften gespeichert. Wenn der Computerschutz aktiviert ist, erstellt Windows automatisch Schattenkopien von Dateien, die seit dem letzten Wiederherstellungspunkt, also in der Regel seit einem Tag, geändert wurden. Wenn die Festplatte partitioniert ist oder wenn mehrere Festplatten im Computer installiert sind, müssen Sie den Computerschutz auch auf den anderen Partitionen oder Festplatten aktivieren.

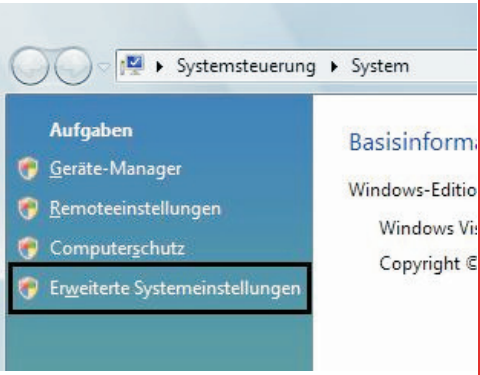
Klicken Sie mit der rechten Maustaste auf die Datei bzw. den Ordner, und klicken Sie dann auf Vorherige Versionen wiederherstellen.

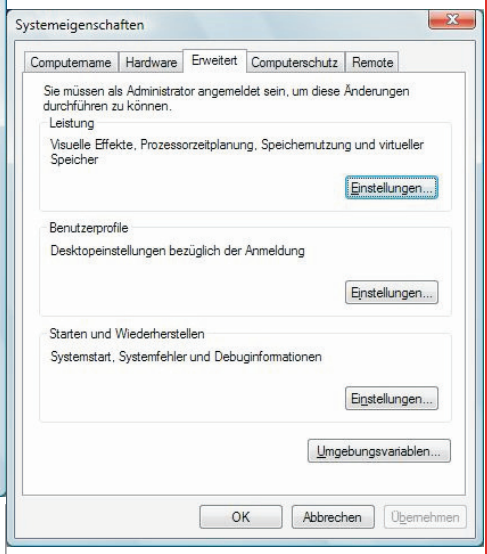
Es wird eine Liste der verfügbaren vorherigen Datei- oder Ordnerversionen angezeigt. Die Liste enthält sowohl Sicherungs- als auch Schattenkopien, sofern beide Typen vorhanden sind.



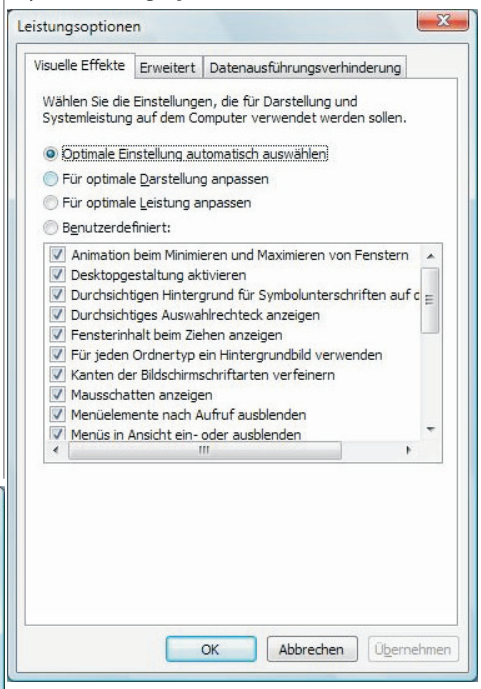
Die Systemeigenschaften von Windows Vista

Aufrufen mit *„Windows-Taste/PAUSE"* oder in der Systemsteuerung.



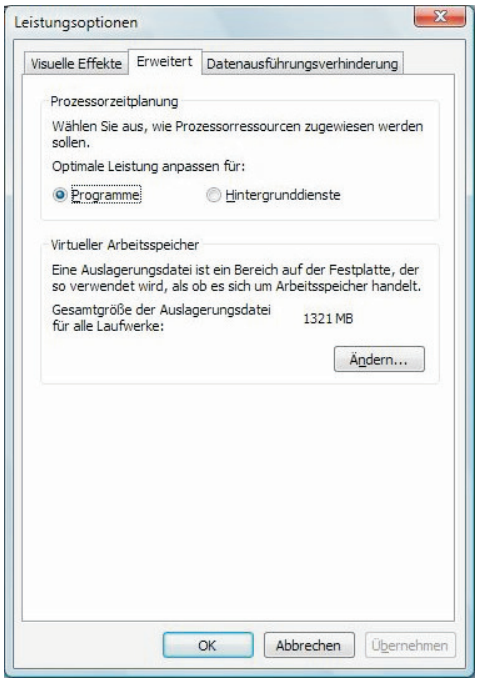


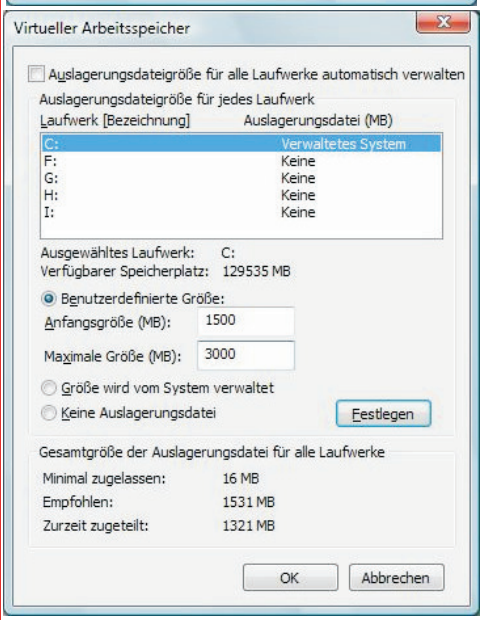
Systemleistungsoptionen



Durch Klick auf *"Ändern"* kann der virtuelle Arbeitsspeicher (d.h. Größe der Auslagerungsdatei, engl. *Swap File*) geändert werden.

Empfohlene Größe der Auslagerungsdatei: etwa 1,5x des installierten Hauptspeichers (mehr hat keinen Sinn, da sonst Performance-Verluste auftreten!). Braucht man mehr, so ist es sinnvoller, physischen Speicherplatz zu ergänzen.





Windows NT-Betriebssysteme unterstützen einen 32-Bit-Adressraum, das bedeutet einen virtuellen Adressbereich von 4 GB. Jedem Programm wird ein solcher virtueller 4 GB-Adressraum zugeordnet. (Hätte man diesen Speicher auch physikalisch, so könnte das Programm diesen Speicher auch nutzen!)

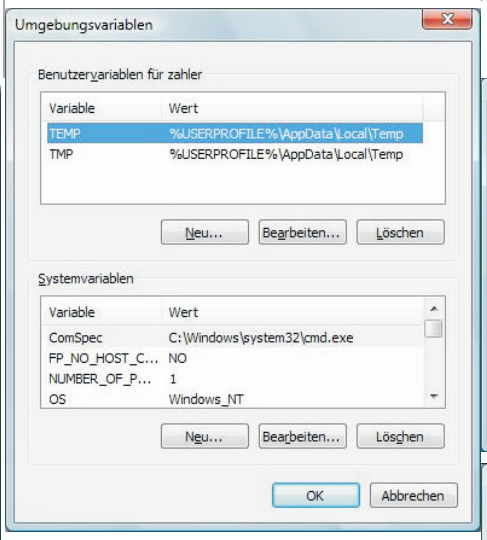
Die Zuordnung zwischen tatsächlich vorhandenem Speicher und virtuellem Speicher wird vom VMM = *Virtual Memory Manager* durchgeführt.

Ist für mehrere Programme eine Zuweisung von tatsächlichem RAM nicht mehr möglich (*Page Fault* = Seitenzuordnungsfehler), so muss ein Teilbereich aus dem RAM auf die Festplatte ausgelagert werden. Damit werden diese Daten auf die "Swap-Datei" (Auslagerungsdatei) auf die Festplatte ausgelagert.

Die Auslagerung erfolgt generell in 4 KB-Blöcken.

Umgebungsvariablen

Altes Konzept, mit dem Programme (älteren Datums) gesteuert werden können.



Die Umgebungsvariablen können in der Kommandozeile abgefragt werden:

```
echo %ComSpec%
```

Diese Variablen können auch gesetzt werden:

```
set werbinich=Zahler
echo %werbinich%
```

Mit `set` können alle Umgebungsvariablen ausgelesen werden:

```
C:\Users\zahler>set
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\zahler\AppData\Roaming
CommonProgramFiles=C:\Program Files\Common
Files
COMPUTERNAME=PC01
ComSpec=C:\Windows\system32\cmd.exe
FP_NO_HOST_CHECK=NO
HOMEDRIVE=Z:
HOMEPATH=\
HOMESHARE=\\dc01\user\zahler\home
LOCALAPPDATA=C:\Users\zahler\AppData\Local
LOGONSERVER=\\DC01
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\Windows\system32;C:\Windows;C:\Windows\
System32\Wbem;C:\Program Files\Wi
ndows Imaging\
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;
.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 15 Model 4
Stepping 9, GenuineIntel
PROCESSOR_LEVEL=15
PROCESSOR_REVISION=0409
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files
PROMPT=$P$G
PUBLIC=C:\Users\Public
SESSIONNAME=Console
SystemDrive=C:
SystemRoot=C:\Windows
TEMP=C:\Users\zahler\AppData\Local\Temp
TMP=C:\Users\zahler\AppData\Local\Temp
USERDNSDOMAIN=ZAHLER.AT
USERDOMAIN=ZAHLER
USERNAME=zahler
USERPROFILE=C:\Users\zahler
windir=C:\Windows
```

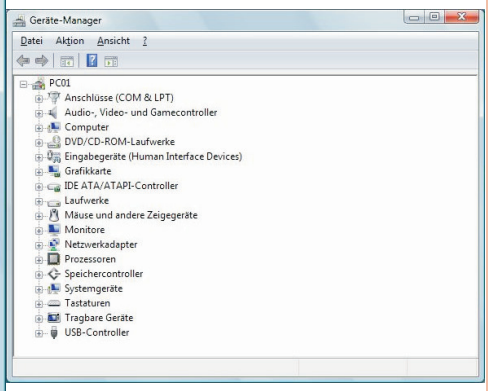
Starten und Wiederherstellen

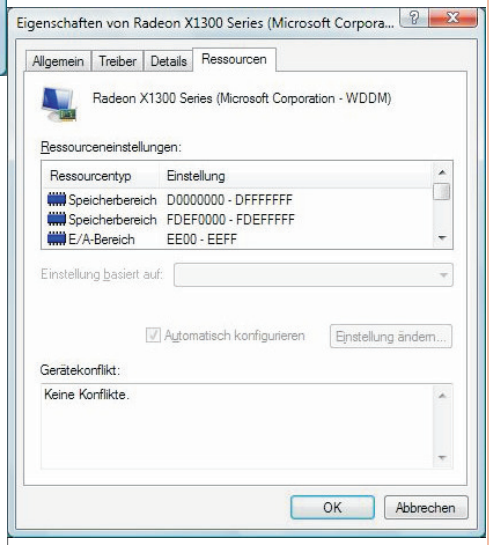
Siehe Kapitel *„Startvorgang"*!

Treiber und Hardware-Installation

Geräte-Manager

Wird meist im Gerätemanager durchgeführt, dieser ist über das Kontextmenü des Arbeitsplatzes erreichbar.



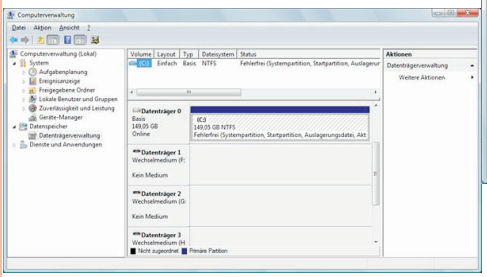


Ressourcenverwaltung:

- IRQ
- E/A-Speicherbereich
- RAM-Speicherbereich
- bei manchen Geräten: DMA-Kanal (zum Beispiel Diskettenlaufwerkscontroller)

Tools zur Verwaltung von Festplatten

Datenträgerverwaltung



Die Betriebssysteme Windows 2000/XP/2003/Vista unterstützen zwei Arten der Festplattenverwaltung:

- **Basisdatenträger:** Hier wird ein zu anderen Systemen kompatibler Master Boot Record erstellt und verwaltet. Daher gibt es für Basisdatenträger die Beschränkung auf max. 4 Partitionseinträge in den MBR. Auf Basisdatenträgern können bootfähige primäre und nicht bootfähige erweiterte Paritionen angelegt werden. Um erweiterte Partitionen für die Datenspeicherung nützen zu können, müssen innerhalb dieser Partitionen noch „logische Laufwerke" definiert werden.
- **Dynamische Datenträger**: Proprietäres Microsoft-System, nicht kompatibel mit anderen Betriebssystemen (auch nicht mit Windows 9x oder NT 4.0). Nur auf dynamischen Datenträgern können RAID- oder übergreifende Laufwerke angelegt werden.

Basisdatenträger können ohne Datenverlust in dynamische Datenträger konvertiert werden; der umgekehrte Vorgang ist aber nicht möglich (es würde eine Neupartitionierung erfolgen, die alle bestehenden Daten unzugänglich macht).

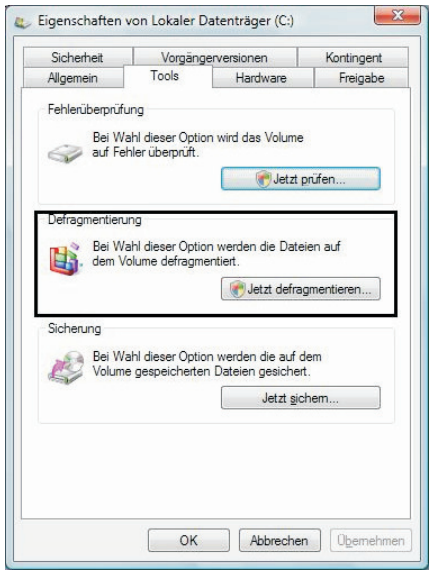
Defragmentierung

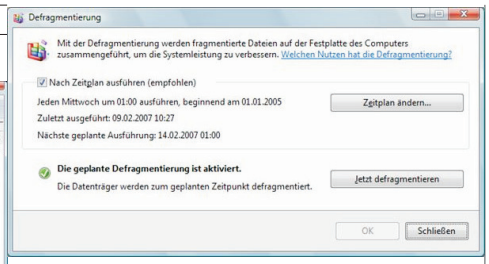
- **Befehlszeilentool** **defrag** (Windows XP/2003)

Syntax:

```
defrag <Volume> [-a] [-f] [-v] [-?]
  Volumelaufwerkbuchstabe oder
Bereitstellungspunkt (d: oder
d:\vol\mountpoint)
  -a      Nur analysieren
  -f      Erzwingt das Defragmentieren auch bei
niedrigem Speicher.
  -v      Ausführliche Ausgabe
  -?      Zeigt die Hilfe an.
```

- **Grafisches Tool**





Partitionierung

- **Befehlszeilentool** `diskpart` (Windows XP/2003)
- **MMC-Snap-In** *„Datenträgerverwaltung"*
- **Drittanbieter-Tools:** Damit sind auch Nicht-Windows-Partitionen (etwa für Multiboot-Umgebungen) einrichtbar.

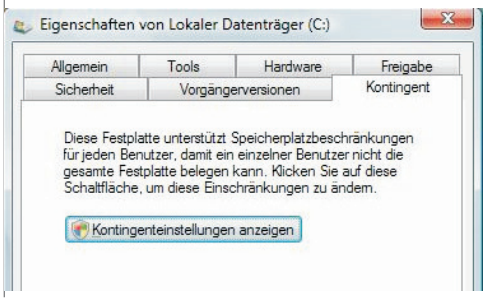
Bekannt ist etwa Symantec PartitionMagic (mit integriertem Bootmanager BootMagic).

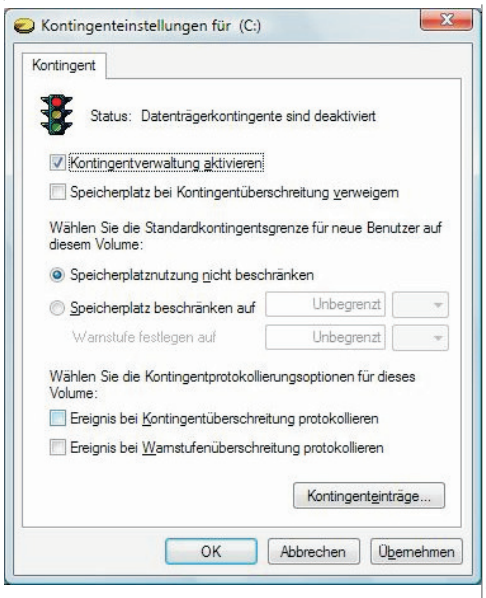
Formatierung

- **Befehlszeilentool** `format`
- **MMC-Snap-In** *„Datenträgerverwaltung"*

Einrichtung von Datenträgerkontingenten (Disk Quota)

- **MMC-Snap-In** *„Datenträgerverwaltung"*





- **Befehlszeilentool** `fsutil` (Windows XP/2003)

Beispiel für die Abfrage von Informationen mit `fsutil`:

```
fsutil fsinfo ntfsinfo C:
NTFS-Volumeseriennummer :
0x94708419708403e8
Version :                          3.1
Anzahl der Sektoren :
0x000000000445c7ae
Gesamtzahl Cluster :
0x0000000000088b8f5
Freie Cluster :
0x00000000007a1800
Insgesamt reserviert :
0x0000000000007f10
Bytes pro Sektor :                 512
Bytes pro Cluster :                4096
Bytes pro Dateidatensatzsegment :  1024
Cluster pro Dateidatensatzsegment : 0
MFT-gültige Datenlänge :
0x0000000000d0fc00
MFT-Start-LCN :
0x0000000000c0000
MFT2-Start-LCN :
0x0000000000445c7a
MFT-Zonenstart :
0x0000000000c0ae0
MFT-Zoneende :
0x0000000001d1720
```

RAID *(Redundant Array of Inexpensive Disks)*

Konzept

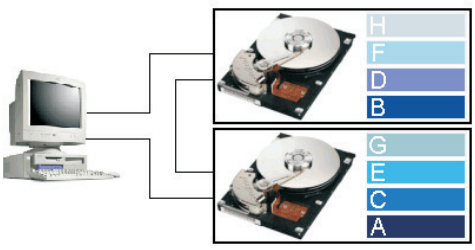
Wächst das Netz, so steigen auch die Anforderungen an Sicherheit und Geschwindigkeit der Massenspeicher. Die heutigen Festplatten haben eine MTBF (*mean time between failures*, mittlerer Störabstand) von über 15 Jahren. Die typischen Zugriffszeiten liegen unter 10 ms. Dies bedeutet aber nicht, dass an sich bedingungslos auf diese Massenspeicher verlassen kann. Um nun den Datenzugriff zu beschleunigen und die Datensicherheit zu erhöhen, haben 1987 die Professoren Gibson, Katz und Patterson der Berkeley University den RAID-Standard *(Redundant Arrays of Inexpensive Disks)* definiert. Dieser Standard enthält verschiedene Definitionen, welche die Geschwindigkeit und die Zuverlässigkeit von Massenspeichern erhöhen. Dies geschieht in der Praxis durch überlappende Schreib- und Lesezugriffe.

RAID Level 0: Block Striping

Block Striping bedeutet, dass einzelne Datenblocks über mehrere Disks verteilt werden, also quasi in "Streifen" zerlegt werden. So kann z.B. eine 20 GB Festplatte in vier Teile zu je 5 GB aufgeteilt werden, so dass die Daten wie folgt verteilt sind:

Die Blockgröße (Striping Depth) beträgt in den meisten Fällen 8kB, kann jedoch von 2 bis 32 kB gehen. Dateien, die größer als 8 kB sind, werden automatisch auf mehrere Disks aufgeteilt. Je nach gewählter Implementation werden mehrere kleine Files in einen Block (Speicheroptimierung) oder jedes File immer in einem eigenen block (Geschwindigkeitsoptimierung) abgelegt. Fällt allerdings ein Laufwerk aus, so sind in aller Regel die dort gespeicherten Segmente verloren und somit die Daten des gesamten Arrays unbrauchbar. Deshalb trägt RAID Level 0 den Namen *Redundant Array* eigentlich zu Unrecht, da die Daten nicht mehrfach gespeichert werden und das Array somit keine Fehlertoleranz bietet. RAID 0 ist für Anwendungen interessant, bei denen ein hoher Datendurchsatz benötigt wird, ohne dass dabei die kontinuierliche Sicherheit von besonderer Bedeutung ist.

RAID 0 (Striping)



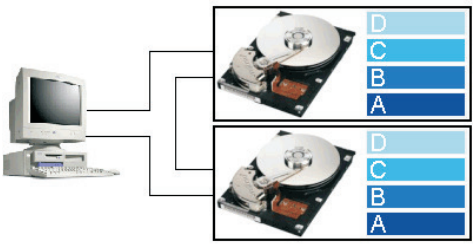
© tecChannel.de

RAID Level 1: Disk Mirroring bzw. Disk Duplexing

Disk Mirroring bedeutet, dass zwei oder mehrere Disks genau dieselben Daten enthalten. Dabei wird aber der gleiche Controller verwendet. Wenn sowohl Controller als auch Disks doppelt vorhanden sind, so wird das so genannte *Disk Duplexing* realisiert:

Jede Information ist also doppelt auf den Festplatten gespeichert, wodurch sich die Schreibvorgänge etwas verlängern. Die Verteilung (bzw. die Verdoppelung) der Daten wird dabei wie folgt vorgenommen:

RAID 1 (Mirroring)



Das Lesen von Daten kann auf verschiedene Arten vonstatten gehen:

- Alle Daten werden von der ersten Disk gelesen, währen die zweite Disk nur als Backup-Disk dient.
- Die Daten werden alternierend von einer oder von der anderen Disk gelesen.
- Eine Leseanfrage wird an alle Disks geleitet; die erste antwortende Disk wird berücksichtigt. (Diese Vorgehensweise wurde von Novell bis zur NetWare Version 3.1 implementiert.)
- Die Daten werden normalerweise von der ersten Disk gelesen. Ist diese beschäftigt, so kommt die zweite Disk zum Zuge. (Diese Vorgehensweise ist von Novell in den Versionen 3.11 und 3.12 sowie 4.x implementiert.)

Beim Schreiben der Daten unter RAID 1 gibt es ebenfalls verschiedene Möglichkeiten:

- Die erste Disk wird sofort beschrieben, während die zweite Disk erst dann einen Schreibauftrag erhält, wenn sie nicht mehr beschäftigt ist.
- die Daten werden sofort auf beide Disks geschrieben; sobald beide Disks fertig sind, geht die Verarbeitung weiter. Diese zwar etwas langsamere Art bietet eine hohe Datensicherheit (wird von NetWare angewendet).

Obwohl RAID 1 die Verdoppelung der Speicherkapazität und damit der Kosten bedeutet, handelt es sich dabei um die am häufigsten implementierte Variante. In der Tat funktioniert RAID 1 bereits mit zwei Festplatten.

Dabei setzt RAID auf eines der ältesten Verfahren zur Fehlerkorrektur, die Paritätsprüfung. Dazu verknüpft es die Daten der Nutzlaufwerke über eine logische Exklusiv-Oder-Operation (XOR) und speichert das Resultat auf einem eigenen Parity-Laufwerk. Das Ergebnis der Verknüpfung ist dann 1, wenn eine ungerade Anzahl von Bitstellen eine 1 aufweist. Bei einer geraden Anzahl dagegen ist das Ergebnis 0:

Parity-Generierung

Laufwerk	Inhalt
Laufwerk A	11101100
Laufwerk B	10110011
Laufwerk C	01001101
Parity-Laufwerk	00010010

Fällt nun ein beliebiges Laufwerk aus, lassen sich durch ein erneutes XOR die verloren gegangenen Daten problemlos rekonstruieren:

Fehlerkorrektur durch Parity

	vor dem Ausfall	Ausfall Datenlaufwerk	Ausfall Parity-Laufwerk
Laufwerk A	11101100	11101100	11101100
Laufwerk B	10110011	xxxxxxx	10110011
Laufwerk C	01001101	01001101	01001101
Parity-Laufwerk	00010010	00010010	xxxxxxx
Datenrekonstruktion		10110011	00010010

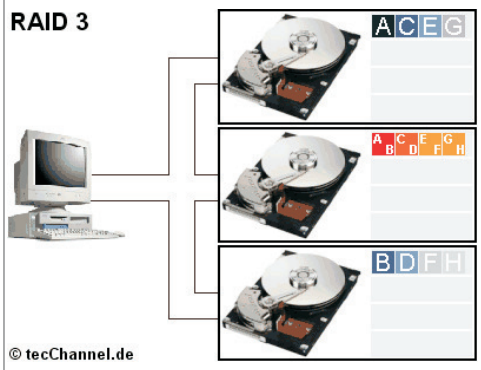
RAID Level 2: Interleaving

Bei dieser Variante von RAID werden die Daten nach dem Interleaving-Verfahren gespeichert. Das erste Segment einer Datei wird auf der ersten Festplatte abgelegt, das zweite Segment auf der zweiten und so weiter. Parallel dazu enthaltene mehrere zusätzliche Platten Prüfnummern und Zusatzinformationen, die im Notfall zur Rekonstruktion der Daten notwendig sind. RAID Level 2 hat im Netzwerkbereich praktisch keine Bedeutung und wird nur auf Großrechnern verwendet; aus diesem Grund wird auf eine weitergehende Darstellung verzichtet.

RAID Level 3: Synchronised Spindles

Bei RAID 3 arbeiten alle Festplatten parallel (synchronisiert). Eine separate Festplatte wird für die Paritätsinformationen verwendet, die im Notfall die Rekonstruktion der Daten erlaubt. So kann bei Ausfall einer Platte die Information mit Hilfe der restlichen Platten rekonstruiert werden.

RAID 3



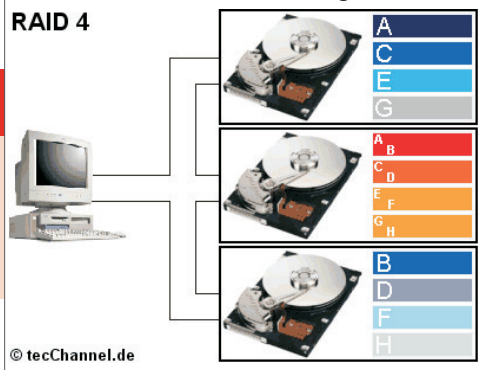
Die Datenübertragungsgeschwindigkeit ist bei RAID 3 bis zu 4 Mal höher als bei einer einzelnen Disk, allerdings auf Kosten der Lesegeschwindigkeit, da die Steuerung immer nur einen Lesebefehl abarbeiten kann. Da die Dateien in kleinen Teilen über alle Platten verteilt sind, ist RAID 3 interessant für Anwendungen mit wenigen, aber sehr großen Dateien (z.B. Graphik, große Datenbanken, etc.). Für häufigen Zugriff auf kleine Dateien oder für intensiven Multitaskingbetrieb sollte RAID 3 nicht angewendet werden, da ein Lesevorgang alle Festplatten blockiert.

RAID Level 4: Block Striping with Parity

Raid Level 4 entspricht RAID 0 mit zusätzlicher Parity. Dies bedeutet, dass die einzelnen Datenblocks über mehrere Disks verteilt werden und eine zusätzliche Disk für die Paritätsinformationen eingesetzt wird.

Die Lesegeschwindigkeit ist dieselbe wie bei RAID 0 und theoretisch vier Mal schneller der einen einzelnen Festplatte. Die Schreiboperationen erfolgen jedoch relativ langsam, da das System nur einen Schreibvorgang nach dem anderen abarbeiten kann und zum Errechnen der Paritätsinformationen zuerst die Daten gelesen werden müssen. RAID 4 eignet sich da-

RAID 4

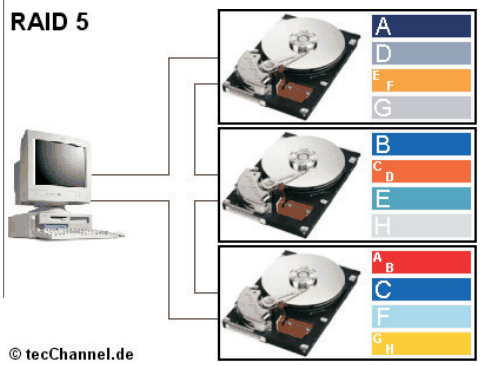


her für Anwendungen, bei denen viel gelesen, aber wenig geschrieben wird.

RAID Level 5: Block Striping with Distributed Parity

RAID 5 begegnet dem Problem der langsamen Schreibvorgänge unter RAID 4 mit dem Schreiben der Paritätsinformationen auf allen Disks (selbstverständlich werden die Daten nicht auf der gleichen Festplatte abgelegt wie die Paritätsinformationen):

RAID 5



RAID 5 wird unter Windows NT/2000 relativ häufig eingesetzt, da es prozentual weniger Speicher „vergeudet" und zudem für Lesevorgänge eine erhöhte Performance bietet.

RAID Level 6/7: Block Striping and Block Mirroring (Exoten, sind unbedeutend)

RAID 6 stellt einen Versuch dar, gegenüber RAID 3 bis 5 die Ausfallsicherheit nochmals zu erhöhen. Bei diesen Verfahren darf nur eine Platte des Arrays ausfallen, da sich sonst die Daten nicht mehr per XOR rekonstruieren lassen. RAID 6 umgeht diese Einschränkung, indem es quasi ein RAID 5 um eine zusätzliches Parity-Laufwerk ergänzt. Zwar dürfen nun zwei Platten des Verbunds ausfallen, ohne dass Datenverluste auftreten. Die zusätzliche Sicherheit muss allerdings mit gegenüber RAID 3 bis 5 deutlich langsameren Schreibzugriffen erkauft werden.

Auch das proprietäre RAID 7 ist ähnlich wie RAID 5 aufgebaut. Allerdings setzt der Hersteller Storage Computer im Controller zusätzlich ein lokales Echtzeitbetriebssystem ein. Schnelle Datenbusse und mehrere große Pufferspeicher koppeln die Laufwerke vom Bus ab. Dieses asynchrone Verfahren soll Lese- wie Schreiboperationen gegenüber anderen RAID-Varianten erheblich beschleunigen. Zudem lässt sich, ähnlich wie bei RAID 6, die Paritätsinformation auch auf mehrere Laufwerke speichern.

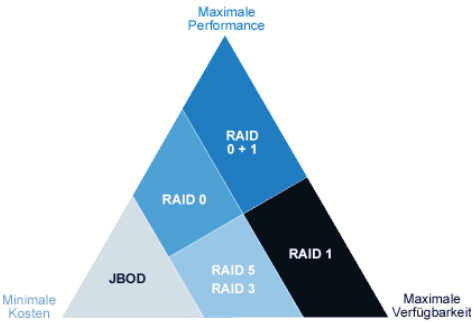
Einsatz

Für den Einsatz der RAID-Technologie spricht, dass mehrere kleine Festplatten schneller sind als eine große Festplatte. Allerdings ist ein sol-

ches System störungsanfälliger, weshalb spezielle Sicherheitsmaßnahmen getroffen werden müssen. In keinem Fall darf aber ein RAID-System als Ersatz für einen regelmäßigen Backup angesehen werden. Grundsätzlich gilt, dass Data Striping die Leistungsfähigkeit stark verbessern kann, während! Data Duplexing den besten Datenschutz bietet. Neben den oben angesprochenen Hardwarelösungen gibt es für gewisse Fälle auch Softwarelösungen, die aber hier nicht weiter besprochen werden sollen.

Welcher RAID-Level gewählt werden soll, hängt von der Menge und Art der zu speichernden Daten ab. Folgende Fragen sollten gestellt werden:

- Wie wichtig – d.h. sicherheitsrelevant – sind Daten?
- Wie oft muss auf die Daten zugegriffen werden?
- Handelt es sich um wenige große oder viele kleine Dateien?



© tecChannel.de

Die folgende Tabelle enthält einen Überblick über die verschiedenen Levels; als Vergleichsgröße beim Schreiben, Lesen und notwendigen Speicherplatz dient eine einfache Festplatte, während bei den Anwendungen die Eignung angegeben wird („+" oder „++" heißt schneller bzw. geeignet, „-„ oder „- -„ heißt langsamer bzw. ungeeignet).

Level	Schreibvorgänge	Lesevorgänge	gebotene Sicherheit	Zusätzlicher Speicherplatz	Komplexe Anwendungen
Festplatte	0	0	--		++
RAID 0	++	++	--	gleich	++
RAID 1	+	+	++	doppelte Kapazität	+
RAID 2	--	++	++	mind. 2 Zusatzplatten	--
RAID 3	+	--	++	eine Zusatzplatte	--
RAID 4	-	++	++	eine Zusatzplatte	++
RAID 5	+	++	++	eine Zusatzplatte	++
RAID 6	++	++	++	doppelte Kapazität	+

Unabhängig vom gewählten Level sollten moderne RAID-Systeme über zusätzlichen Sicherheits- und Überwachungsmechanismen verfügen. Solche Mechanismen umfassen beispielsweise die Möglichkeit des *„Hot Mounting"* (Austausch im laufenden Betrieb) und der laufenden Überprüfung des Zustandes der Festplatten. Ein weiteres Merkmal von modernen RAID-Systemen ist die Integration von eigenem Cache-Speicher, der die Leistungsfähigkeit stark erhöhen kann.

RAID-Implementierungen in Windows 2000/XP/2003

Um den Zugriff auf Daten bei Ausfall einer Festplatte zu erhalten, bietet Windows 2000 Server eine Softwareimplementierung einer Fehlertoleranztechnologie, die RAID *(Redundant Array of Independent Disks)* genannt wird. RAID stellt eine Fehlertoleranz durch die Implementierung einer Datenredundanz bereit. Die Datenredundanz sorgt dafür, dass ein Computer Daten auf mehr als einen Datenträger schreibt, wodurch die Daten bei Ausfall einer der Festplatten geschützt sind.

Sie können die RAID-Fehlertoleranz als Software- oder Hardwarelösung implementieren.

Software-RAID-Implementierungen

Windows 2000 Server unterstützt zwei Softwareimplementierungen von RAID: gespiegelte Datenträger (RAID 1) und Stripesetdatenträger mit Parität (RAID 5). Sie können neue RAID-Datenträger jedoch nur auf dynamischen Festplatten von Windows 2000 erstellen.

Bei Softwareimplementierungen von RAID ist eine Fehlertoleranz nach einem Ausfall erst möglich, wenn der Fehler behoben wurde. Tritt ein zweiter Fehler auf, ehe die Daten des ersten Fehlers wiederhergestellt wurden, können Sie die Daten nur aus einer Sicherung wiederherstellen.

Anmerkung: Bei einer Aktualisierung von Windows NT 4.0 auf Windows 2000 werden vorhandenen gespiegelte Datenträger und Stripesets mit Parität beibehalten. Windows 2000 bietet eine eingeschränkte Unterstützung dieser Fehlertoleranzsätze, d.h. sie können diese verwalten und löschen.

Alle RAID-Implementierungen von Windows 2000/2003 setzen dynamische Datenträger voraus!

Hardware-RAID-Implementierungen

Bei einer Hardwarelösung ist der Datenträgercontroller für das Erstellen und Wiederherstellen redundanter Informationen verantwortlich. Einige Hardwarehersteller implementieren einen RAID-Datenschutz direkt in ihre Hardware, z.B. mit Hilfe von Controllerkarten für Datenträgersätze. Da diese Methoden herstellerspezifisch sind und die Treiber der Fehlertoleranzsoftware des Betriebssystems umgehen, sind sie leistungsfähiger als Softwareimplementierungen von RAID. Darüber hinaus bieten Hardware-RAID-Implementierungen weitere Funktionen, wie z.B. zusätzliche fehlertolerante RAID-Konfigurationen, den Austausch fehlerhafter Festplatten im laufenden Betrieb, Reservelaufwerke für die Online-Umschaltung im Fehlerfall und dedizierten Zwischenspeicher zur Verbesserung der Leistung.

Anmerkung: Der in einer Hardwareimplementierung unterstützte RAID-Grad ist abhängig vom Hardwarehersteller.

Berücksichtigen Sie bei einer Entscheidung für eine Software- oder Hardware Implementierung von RAID die folgenden Punkte:

- Hardwarefehlertoleranz ist teurer als Softwarefehlertoleranz.
- Hardwarefehlertoleranz bietet in der Regel eine schnellere Datenträger-E/A als Softwarefehlertoleranz.
- Hardwarefehlertoleranzlösungen können die Geräteoptionen auf einen einzelnen Hersteller beschränken.
- Hardwarefehlertoleranzlösungen ermöglichen u.U. den Austausch von Festplatten bei laufendem Betrieb, ohne dass der Computer heruntergefahren werden muss, und Reservelaufwerke, die bei einem Fehlerfall automatisch aktiviert werden.

Gespiegelte Datenträger

Ein gespiegelter Datenträger nutzt den Fehlertoleranztreiber von Windows 2000/2003 Server (`ftdisk.sys`), um dieselben Daten gleichzeitig auf je ein Laufwerk auf zwei physischen Festplatten zu schreiben. Die beiden Laufwerke werden als Mitglieder des gespiegelten Datenträgers betrachtet. Das Implementieren eines gespiegelten Datenträgers sorgt für den Erhalt von Daten, wenn ein Mitglied des gespiegelten Datenträgers fehlerhaft sein sollte.

Ein gespiegelter Datenträger kann beliebige Partitionen enthalten, einschließlich der Start- oder Systempartition. Die Laufwerke eines gespiegelten Datenträgers müssen jedoch dynamische Windows 2000/2003-Laufwerke sein.

Gespiegelte Datenträger können als Stripesets auf mehrere Laufwerke verteilt werden. Diese Konfiguration wird häufig RAID 10 genannt, RAID 1 (Spiegelung) und RAID 0 (Striping). Im Gegensatz zu RAID 0 ist RAID 10 eine fehlertolerante RAID-Konfiguration, da jeder Datenträger im Stripeset auch gespiegelt wird. RAID 10 verbessert die Datenträger-E/A, indem Lese- und Schreibvorgänge im gesamten Stripeset ausgeführt werden.

Leistung gespiegelter Datenträger

Gespiegelte Datenträger können die Leseleistung verbessern, da der Fehlertoleranztreiber Daten beider Mitglieder des Datenträgers gleichzeitig liest. Die Schreibleistung ist geringfügig schwächer, da der Fehlertoleranztreiber Daten auf beide Mitglieder schreiben muss. Fällt eines der Laufwerke eines gespiegelten Datenträgers aus, bleibt die Leistung normal, da der Fehlertoleranztreiber nur in einer Partition arbeitet.

Da die Speichernutzung nur 50 % beträgt (da die Daten auf beiden Mitgliedern doppelt vorhanden sind), können gespiegelte Datenträger kostenintensiv sein.

Achtung: Beim Löschen eines gespiegelten Datenträgers werden alle Informationen auf diesem Datenträger gelöscht.

Diskduplexing

Wenn beide physischen Laufwerke eines gespiegelten Datenträgers vom selben Controller gesteuert werden und der Controller ausfällt, kann auf kein Mitglied des gespiegelten Datenträgers zugegriffen werden. sie können einen zweiten Controller in den Computer einbauen, sodass jedes Laufwerk des gespiegelten Datenträgers über einen eigenen Controller verfügt. Diese Konfiguration, die Diskduplexing genannt wird, kann den gespiegelten Datenträger vor Controller- und Festplattenausfällen schützen. Verschiedene Hardwareimplementierungen von Diskduplexing verwenden auf einer einzelnen Festplattencontrollerkarte zwei oder mehrere Kanäle.

Durch Diskduplexing werden der Busverkehr reduziert und die Leseleistung u. U. gesteigert. Diskduplexing ist eine Hardwareerweiterung eines gespiegelten Windows 2000-Datenträgers, für die keine weitere Softwarekonfiguration erforderlich ist.

RAID 5-Datenträger

Windows 2000 Server unterstützt ferner die Fehlertoleranz mittels Stripesetdatenträgern mit Parität (RAID 5). Die Parität ist ein mathematisches Verfahren zur Bestimmung der Anzahl gerader und ungerader Bits in einem Wert oder einer Wertfolge, mit dem Daten rekonstruiert werden können, wenn ein Wert in einer Wertfolge verlogen gegangen ist.

Bei einem RAID 5-Datenträger erzieht Windows 2000 die Fehlertoleranz dadurch, dass jeder Laufwerkpartition des Datenträgers ein sog. Stripe mit Paritätsinformationen hinzugefügt wird (siehe Abbildung 12.12). Falls ein Laufwerk ausfällt, kann Windows 2000 die Daten und Paritätsinformationen auf den verbleibenden Laufwerken verwenden, um die Daten auf dem ausgefallenen Laufwerk zu rekonstruieren.

Aufgrund der Paritätsberechnung sind Schreibvorgänge auf einem RAID 5-Datenträger langsamer als auf einem gespiegelten Datenträger. RAID 5-Datenträger bieten jedoch eine bessere Leseleistung als gespiegelte Datenträger, insbesondere mit mehreren Controllern, da die Daten auf mehrere Laufwerke verteilt sind. Wenn hingegen ein Laufwerk ausfällt, verlangsamt sich die Leseleistung eines RAID 5-Datenträgers solange, bis Windows 2000 Server die Daten auf dem ausgefallenen Laufwerk mit Hilfe der Paritätsinformationen rekonstruiert hat.

RAID 5-Datenträger haben gegenüber gespiegelten Datenträgern einen Kostenvorteil, da die Speicherplatznutzung optimiert wird. Je mehr Laufwerke in einem RAID 5-Datenträger vorhanden sind, desto geringer sind die Kosten für den redundanten Datenstripe. Die folgende Tabelle zeigt, wie der für den Datenstripe benötigte Speicherplatz gesenkt wird, wenn dem RAID 5-Datenträger 2-GB-Festplatten hinzugefügt werden.

Anz.d. Laufwerke	Belegter Speicherplatz	Verfügbarer Speicherplatz	Redundanz
3	6 GB	4 GB	33 %
4	8 GB	6 GB	25 %
5	10 GB	8 GB	20 %

Bei Software-RAID 5-Datenträgern gelten folgende Einschränkungen. Erstens umfassen RAID-5-Datenträger mindestens drei und höchstens 32 Festplattenlaufwerke. Zweitens darf ein Software-RAID 5-Datenträger keine Start- oder Systempartition enthalten.

Für das Betriebssystem Windows 2000 stellen Hardware-RAID-Implementierungen keine Besonderheit dar. Aus diesem Grund gelten die Einschränkungen von Software-RAID-Konfigurationen nicht für Hardware-RAID-Konfigurationen.

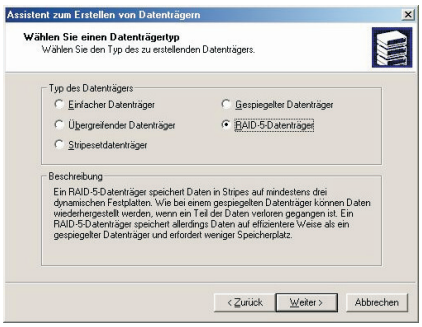
Gespiegelte und RAID 5-Datenträger – Vergleich

Gespiegelte und RAID 5-Datenträger bieten einen unterschiedlichen Grad an Fehlertoleranz. Die Auswahl der zu implementierenden Lösung hängt vom Grad des benötigten Schutzes und den Hardwarekosten ab. Die Hauptunterschiede zwischen gespiegelten Datenträgern (RAID 1) und RAID 5-Datenträgern liegen bei Leistung und Kosten. Die folgende Tabelle erklärt Unterschiede zwischen den Softwareimplementierungen von RAID 1 und RAID 5.

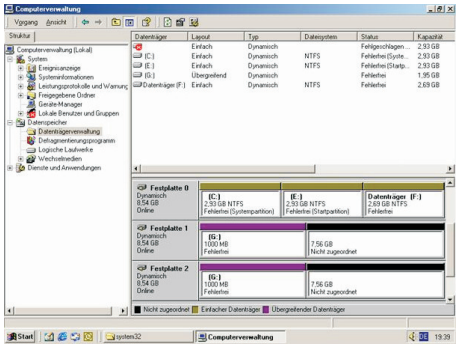
Gespiegelte Datenträger RAID 1	Stripesetdatenträger mit RAID 5
Unterstützen FAT und NTFS	Unterstützten FAT und NTFS
Können System- oder Startpartition schützen	Können System- oder Startpartition nicht schützen
Benötigen zwei Festplatten	Benötigen mindestens drei Festplatten und maximal 32 Festplatten
Höhere Kosten pro Megabyte	Niedrigere Kosten pro Megabyte
50 %-ige Speicherbelegung	Mindestens 33 %-ige Speicherbelegung
Gute Schreibleistung	Mittelmäßige Schreibleistung
Gute Leseleistung	Hervorragende Leseleistung
Benötigen weniger Systemspeicher	Benötigen mehr Systemspeicher

Gespiegelte Datenträger bieten in der Regel eine vergleichbare Lese- und Schreibleistung wie einzelfestplatten. RAID 5-Datenträger bieten jedoch eine bessere Leseleistung als gespiegelte Datenträger, insbesondere mit mehreren Controllern, da die Daten auf mehrere Laufwerke verteilt sind. Dadurch, dass die Paritätsinformationen berechnet werden müssen, wird jedoch mehr Arbeitsspeicher benötigt, wodurch sich die Schreibleistung verlangsamen kann.

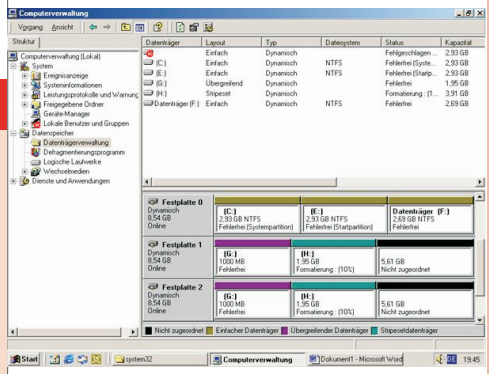
Gespiegelte Datenträger belegen nur 50 % des verfügbaren Speicherplatzes, weshalb die Kosten pro Megabyte (MB) höher sind als bei Laufwerken ohne Spiegelung. Bei Verwendung der Mindestanzahl an Festplatten (drei) belegen RAID 5-Datenträger 33% des verfügbaren Speicherplatzes mit Paritätsinformationen. Werden weitere Festplatten hinzugefügt, wird die Speicherplatzbelegung entsprechend gesenkt.



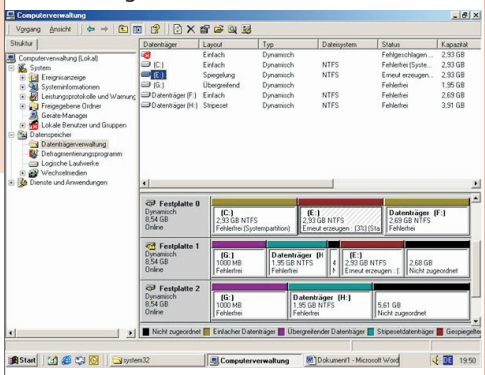
Beispiel: Übergreifender Datenträger = Partition, die auf zwei physische Festplatten verteilt ist (untere Abb: Laufwerk G:)



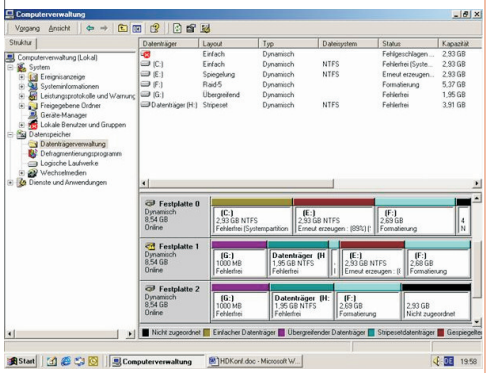
Beispiel: RAID 0 = Stripeset-Datenträger (Laufwerk H:)

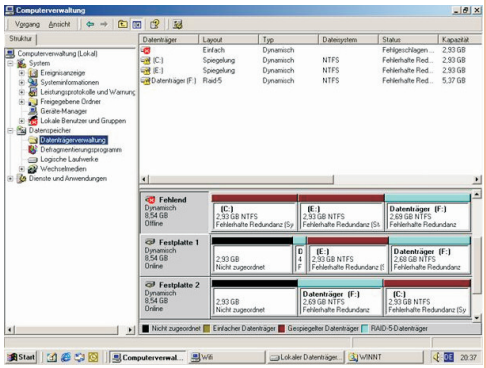


Beispiel: Gespiegelter Datenträger = RAID 1-Datenträger (Laufwerk E:)



Beispiel: RAID 5-Datenträger (Laufwerk F:)





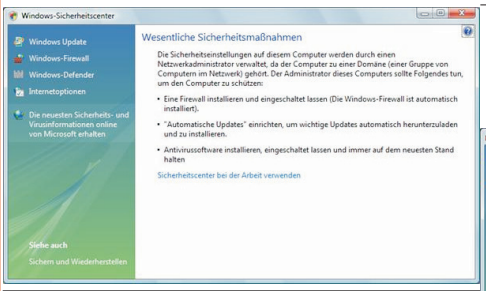
Windows Vista-Sicherheitseinstellungen

In Windows Vista wurden eine Reihe zusätzlicher Sicherheitskonfigurationen eingeführt. Die mit Windows XP SP2 eingeführten Maßnahmen wurden oft erheblich erweitert und verbessert.

Sicherheitscenter

Damit lassen sich maßgebliche Sicherheitseinstellungen bequem verwalten:

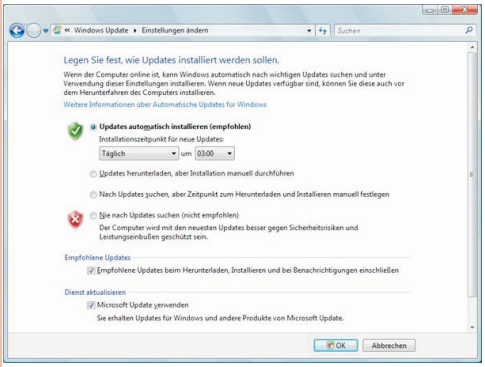
- Windows Update
- Windows-Firewall
- Windows-Defender
- Internetoptionen



Windows Update

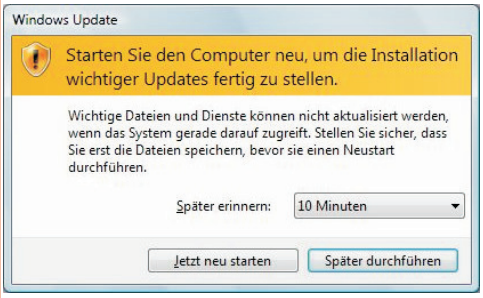
Windows Update sorgt durch die Bereitstellung von Microsoft Windows Vista-Softwareupdates dafür, dass Ihr Computer sicherheitstechnisch auf dem neuesten Stand bleibt. Sie können Windows Update so konfigurieren, dass Updates automatisch heruntergeladen und installiert werden. Sie müssen dieses Feature lediglich aktivieren und brauchen sich anschließend nicht mehr darum zu kümmern.

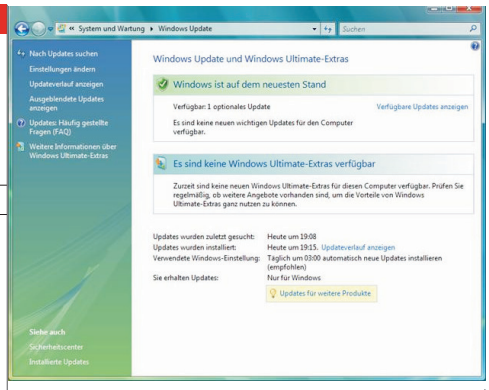
Updates beinhalten Fehlerkorrekturen, Sicherheitspatches und Verbesserungen und sollten daher regelmäßig eingespielt werden.



Unter Windows Vista geht der Funktionsumfang von Windows Update über den von Windows XP gebotenen Funktionsumfang hinaus, wodurch Updates einfacher und störungsfreier erfolgen.

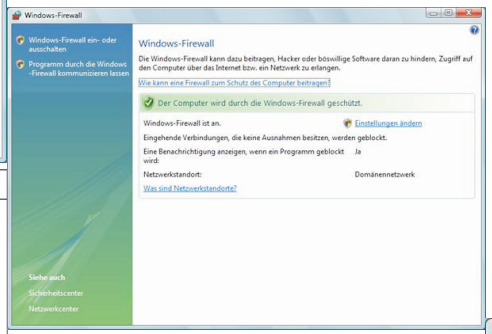
Eine Anpassung der Einstellungen und Aktionen von Windows Update ermöglicht reibungslose Updates und bietet Flexibilität, sobald diese Updates bereitstehen.





Windows Firewall

Die Windows Vista-Firewall sorgt für einen Schutz vor Hackern, Viren und Würmern, die versuchen, aus dem Internet auf Ihren Computer zu gelangen.



Eine Firewall trägt zur Sicherheit des Computers bei. Sie schränkt die Übertragung von Informationen, die von anderen Computern bei Ihrem Computer eingehen, ein, so dass Sie eine bessere Kontrolle über die Daten auf Ihrem Computer haben und besser vor Personen oder Programmen (einschließlich Viren und Würmer) geschützt sind, die unaufgefordert versuchen, eine Verbindung mit Ihrem Computer herzustellen.

Sie können sich eine Firewall wie eine Absperrung vorstellen, die die Daten (häufig auch Verkehr genannt), die aus dem Internet oder einem Netzwerk eingehen, überprüft und diese Daten dann in Abhängigkeit von den Firewalleinstellungen entweder zurückweist oder zum Computer passieren lässt.

In Microsoft Windows Vista ist die Windows-Firewall standardmäßig aktiviert. (Möglicherweise wird sie jedoch von einigen Computerherstellern und Netzwerkadministratoren deaktiviert.) Es ist nicht nötig, die Windows-Firewall zu verwenden; Sie können jeden gewünschten Firewall installieren und ausführen. Informieren Sie sich über die Features anderer Firewalls, und entscheiden Sie dann, welcher Firewall Ihre Anforderungen am besten erfüllt. Wenn Sie sich für die Installation und Ausführung einer anderen Firewall entscheiden, sollten Sie die Windows-Firewall deaktivieren.

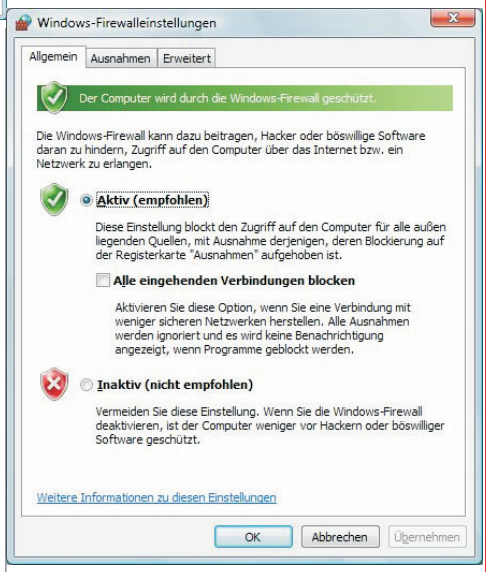
Funktionsweise: Wenn ein Benutzer im Internet oder in einem Netzwerk versucht, eine Verbindung mit Ihrem Computer herzustellen, sprechen wir bei diesem Versuch von einer "unverlangten Anforderung". Wenn eine unverlangte Anforderungen bei Ihrem Computer eingeht, wird die Verbindung von der Windows-Firewall gesperrt. Wenn Sie ein Programm ausführen, z. B. ein Instant Messaging-Programm oder ein Multiplayer-Netzwerkspiel, das auf den Empfang von Daten aus dem Internet oder einem Netzwerk angewiesen ist, werden Sie von der Firewall gefragt, ob die Verbindung gesperrt bleiben oder die Sperrung aufgehoben (d. h. die Verbindung zugelassen) werden soll. Wenn Sie die Sperrung der Verbindung aufheben, erstellt der Windows-Firewall eine Ausnahme, so dass sich der Firewall in Zukunft nicht mehr daran stört, wenn dieses Programm Daten empfangen muss.

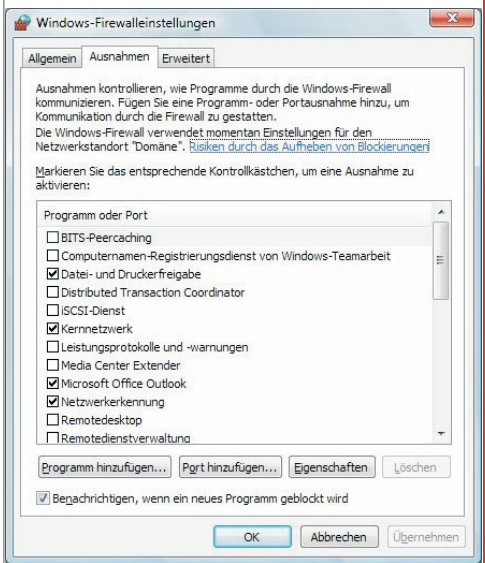
Wenn Sie beispielsweise Sofortnachrichten mit einer anderen Person austauschen, die Ihnen eine Datei (z. B. ein Foto) senden möchte, werden Sie vom Windows-Firewall gefragt, ob Sie die Sperrung für die Verbindung aufheben und den Empfang des Fotos auf Ihrem Computer zulassen möchten. Wenn Sie zusammen mit Freunden ein Multiplayerspiel über das Internet spielen möchten, können Sie das Spiel ebenfalls als Ausnahme hinzufügen, so dass der Firewall den Empfang der Spieledaten auf Ihrem Computer zulässt.

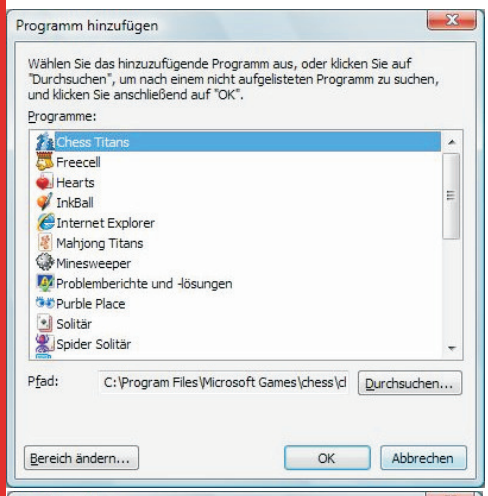
Sie können die Windows-Firewall zwar für bestimmte Internet- und Netzwerkverbindungen deaktivieren, allerdings erhöhen Sie damit das Risiko, dass die Sicherheit des Computers beeinträchtigt wird.

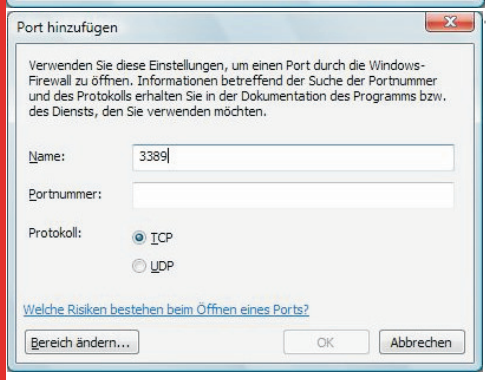
Konfiguration der Windows Firewall

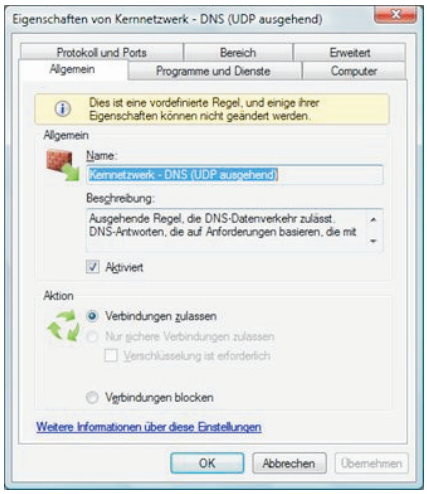
Eigenschaften der LAN-Verbindung oder Systemsteuerung

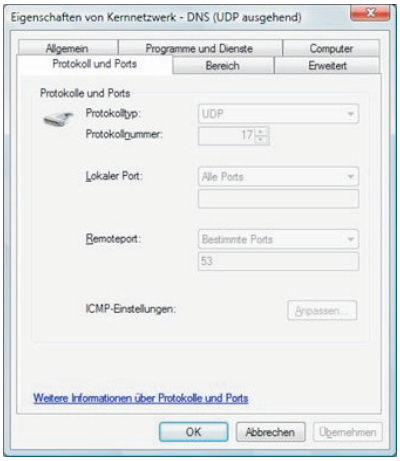






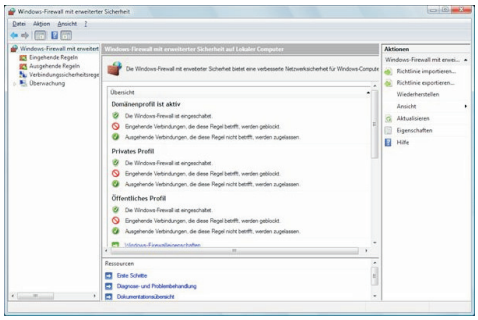


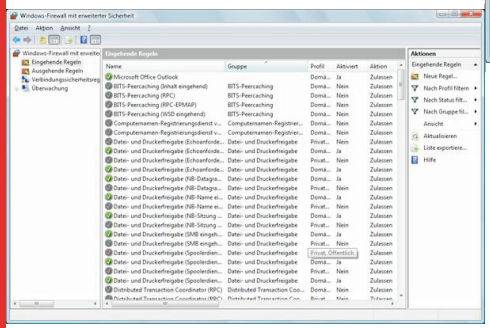




Erweiterte Firewall-Konfiguration

Weitere Details können im Verwaltungsmenü unter „Windows-Firewall mit erweiterter Sicherheit" konfiguriert werden:





Beispiele für benötigte Ports:

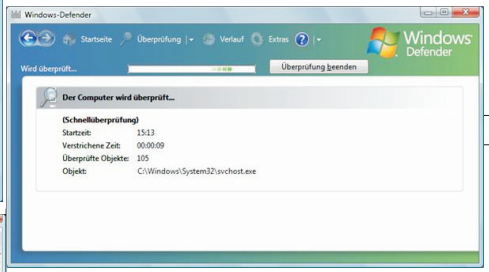
Datei- und Druckerfreigabe: TCP 139, 445, UDP 137, 138

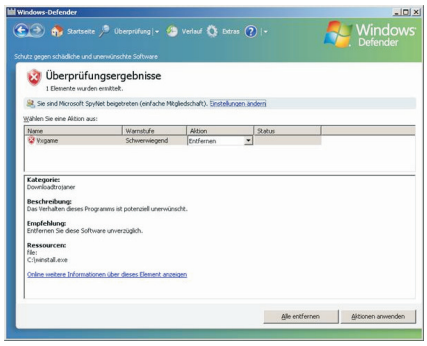
Remote-Desktop: 3389

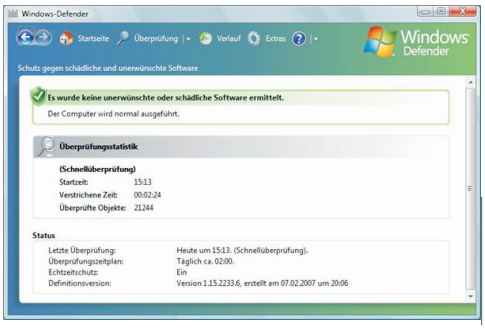
VPN: 1723

Windows Defender

Der Windows-Defender schützt Sie vor Spyware und anderer möglicherweise unerwünschter Software.

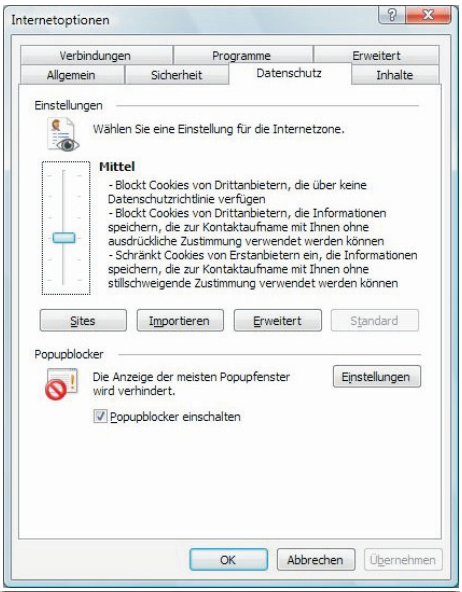


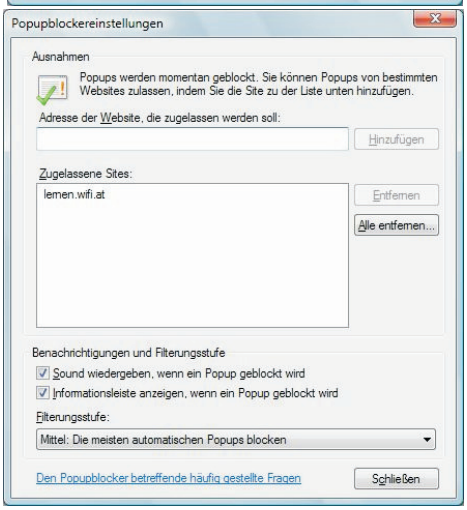




Popup-Blocker

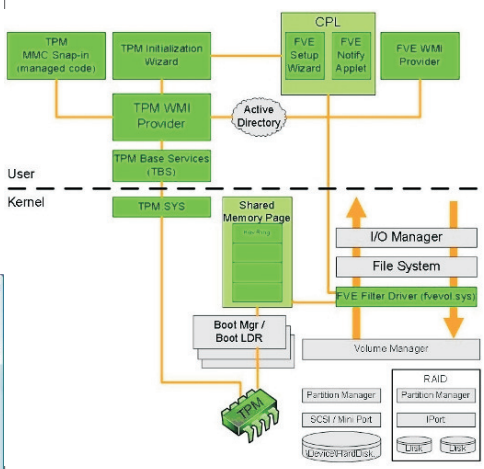
Im Internet Explorer 7 ist der Popup-Blocker standardmäßig aktiviert:





BitLocker

Eine der größten Neuerungen im Business-Bereich ist die Verschlüsselungstechnik rund um BitLocker. Enthalten ist die neue Technologie in den Ultimate- und der Enterprise-Edition sowie der kommenden Server-Version. Das optionale Feature verschlüsselt auf Wunsch die verfügbaren Festplatten. Dabei ist der Schutz bereits während des Bootvorgangs aktiv.

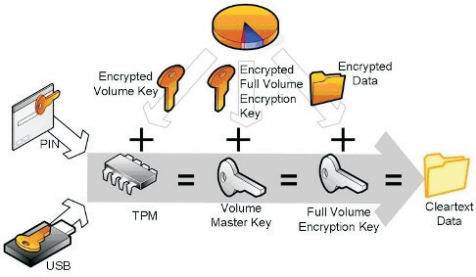


Gesicherte Daten: BitLocker arbeitet mit dem TPM zusammen und schützt so die Daten zuverlässig. (Quelle: Microsoft)

BitLocker verwendet bevorzugt Systeme, die ein *rusted Platform Module* Version 1.2 (TPM 1.2) aufweisen. Der notwendige Chip ist aktuell nur in einzelnen Business-Systemen verbaut, soll aber Bestandteil der kommenden Sicherheitsarchitekturen Presidio (AMD) und LaGrande (Intel) sein.

BitLocker schützt Festplatten sogar nach ihrem aktiven Einsatz. Wenn der Lebenszyklus einer Platte beendet ist, musste sie bisher entweder mechanisch verschrottet oder aufwendig gelöscht werden, um wirklich alle darauf enthaltenen Daten zu beseitigen. Nun reicht es, die entsprechenden Schlüssel zu löschen. Selbst wenn jemand die Festplatten in einen anderen PC einbaut, bleiben die Daten ohne die passenden Zugangsdaten unlesbar.

Die BitLocker-Technologie setzt an zwei Punkten an. Zum einen führt sie bei jedem Bootvorgang eine Integritätsprüfung durch, zum anderen verschlüsselt sie die ausgewählten Festplattenpartitionen.



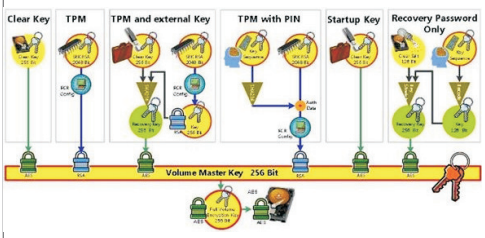
Zutritt verweigert: Nur wenn alle digitalen Schlüssel passen, werden die Daten entschlüsselt. (Quelle: Microsoft)

BitLocker greift dabei auf TPM zurück, um von dem System eine Art Fingerabdruck zu erzeugen. Solange an der eigentlichen Hardware nichts manipuliert wird, bleibt der digitale Fingerabdruck derselbe. Während des Bootvorgangs gleicht BitLocker die Daten ab, erst wenn die beiden Schlüssel übereinstimmen, werden die Daten auf der Festplatte entschlüsselt.

Wahlweise kann der Administrator auch einen PIN oder einen Hash-Key auf einem USB-Stick anfordern lassen, mit dem sich der Nutzer zusätzlich verifizieren muss. Erst wenn alle Schlüssel als gültig anerkannt sind, werden die Daten entschlüsselt, und der Startvorgang wird fortgesetzt.

Die Verschlüsselung der Partitionen macht sich ebenfalls TPM zu Nutze. Zunächst wird die angegebene Partition mit dem Full Volume Encryption Key (FVEK) verschlüsselt; dieser nutzt einen 256-Bit-AES-Algorithmus. Anschließend wird der FVEK erneut verschlüsselt, diesmal mit dem Volume Master Key (VMK), ebenfalls in 256 Bit AES.

Der Volume Master Key wird also als zusätzliche Schicht zwischen dem Anwender und den verschlüsselten Daten eingeführt. Das hat mehrere Vorteile. Der Anwender kommuniziert nie direkt mit dem Basisschlüssel, kann diesen also nicht mitloggen oder auslesen. Wenn die Sicherheit kompromittiert wurde, muss zudem nur der VMK neu erzeugt werden. Ein Ent- und anschließendes Neuverschlüsseln sämtlicher Partitionen mit geändertem Key ist daher nicht notwendig.

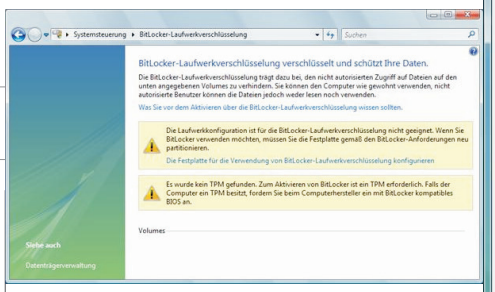


Schlüsselbrett: Der Volume Master Key dient als zentraler Zugangsschlüssel. (Quelle: Microsoft)

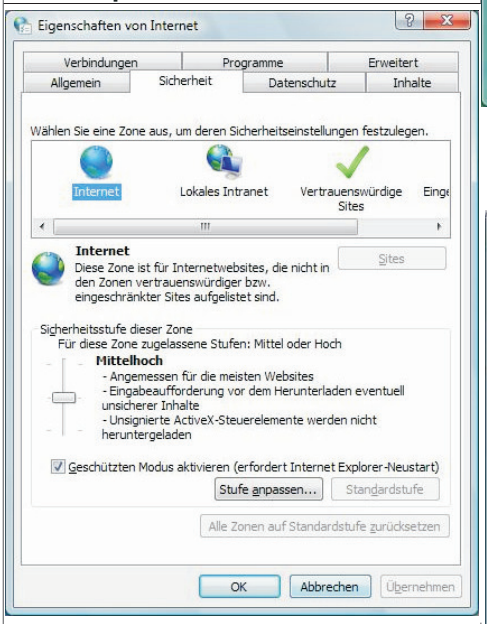
Aus dem VMK schließlich werden alle Schlüsselwerte für den Nutzer und die Recovery-Optionen erstellt. Löscht man also einen kompromittierten VMK, haben alle damit erstellten Schlüssel keinen Zugriff mehr.

IT-Administratoren können BitLocker künftig wahlweise lokal oder per Remote-Zugriff kontrollieren. Neben der Management-Funktion gibt es verschiedene Assistenten und Scripts.

Die konkrete Konfiguration kann über die Systemsteuerung erfolgen; zum optimalen Einstellen des Schutzes ist aber bereits ein spezieller Betriebssystem-Installationsvorgang erforderlich.



Internet- ptionen



Windows-Tool zum Entfernen b sartiger Software

Und das Windows-Tool zum Entfernen bösartiger Software durchsucht Ihren PC regelmäßig auf bekannte weit verbreitete Viren. (Dieses Tool ist keine Komponente von Windows Vista, sondern kann gratis von der Microsoft-Website heruntergeladen werden.)

Virenschutzl sungen

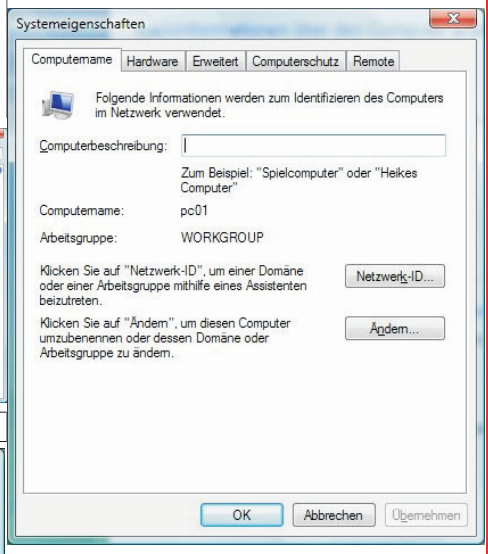
Zusätzlich zu diesen integrierten Windows Vista-Features sollten Sie auf dem Computer eine Virenschutzsoftware wie Windows OneCare oder eine Virenschutzlösung eines Partners von Microsoft aktivieren. Unabhängig von der gewählten Lösung müssen Sie Ihre Virenschutzsoftware regelmäßig aktualisieren. Diese Aktualisierungen werden von den meisten Herstellern von Virenschutzsoftware als Abonnements bereitgestellt.

Im Zusammenspiel können diese Tools Ihren PC vor bösartiger Software schützen.

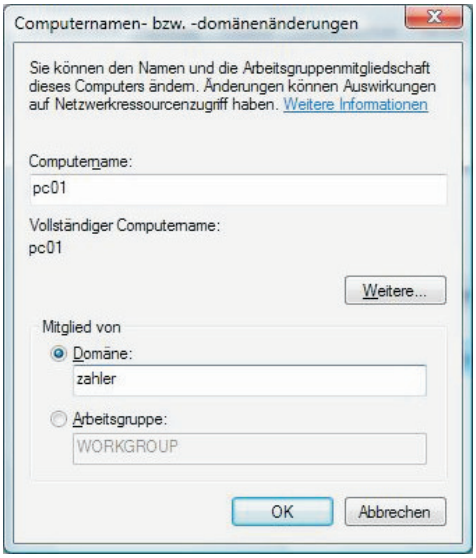
Aufnehmen von Arbeitsstationen in Active Directory-Domänen

Schritt 1 (WICHTIG!): Ändern Sie die IP-Konfiguration der Arbeitsstation so, dass als bevorzugter DNS-Server die IP-Adresse des Domänencontrollers eingestellt wird. (Wir nehmen an, dass der Domänencontroller selbst der für die Domäne zuständige DNS-Server ist.)

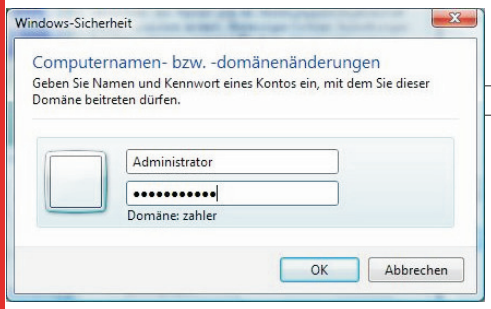
Schritt 2: ffnen Sie die ***Systemeigenschaften*** (***Systemsteuerung*** – System oder Tastenkombination ***Windows-Pause***) und zeigen Sie das Dialogfeld ***„Computername“*** an. Dort klicken Sie auf die Schaltfläche ***„Ändern“***:



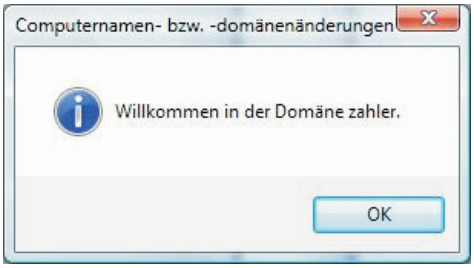
Ändern Sie im folgenden Dialogfeld die Einstellung ***„Mitglied von“*** auf ***„Domäne“*** und geben Sie den NetBIOS-Namen der Domäne an.



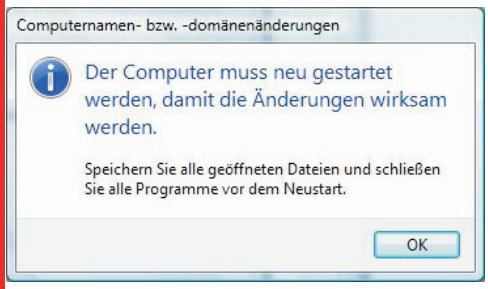
Sie werden nun nach einem Konto gefragt, das in der Lage ist, Computerkonten zum Active Directory hinzuzufügen. Geben Sie hier die Anmeldeinformationen des **Domänenadministrators** an.



Nach einiger Zeit wird der Vorgang mit der Erfolgsmeldung *„Willkommen in der Domäne Domänenname"* bestätigt.



Abschließend muss der Computer neu gestartet werden.



Vorgänge beim Aufnehmen eines Computers in die Domäne:

- Im Active Directory wird ein Computerkonto erzeugt.
- In der AD-integrierten DNS-Zone der Domäne wird ein A-Eintrag (und gegebenenfalls auch ein PTR-Eintrag) für den Computer erzeugt.
- Am Arbeitsstations-PC wird die Sicherheitsgruppe *„Domänen-Admins"* zur lokalen Gruppe *„Administratoren"* hinzugefügt.
- Am Arbeitsstations-PC wird die Sicherheitsgruppe *„Domänen-Benutzer"* zur lokalen Gruppe *„Benutzer"* hinzugefügt. (Überlegen Sie: Warum?)

Vista und mobile Geräte

Windows Vista bietet spezielle Unterstützung für mobile Geräte. Zu den mobilen Geräten gehören:

- Notebooks
- Tablet PCs
- PDAs, vorzugsweise mit Windows Mobile V6

Windows-Mobilitätscenter

Mit dem Windows-Mobilitätscenter können Sie an einem zentralen Ort schnell auf die Einstellungen Ihres mobilen PCs zugreifen. Sie können beispielsweise die Lautsprecherlautstärke Ihres mobilen PCs anpassen, den Status Ihrer drahtlosen Netzwerkverbindung überprüfen und die Helligkeit des Bildschirms anpassen – alles an einem zentralen Ort.

Sie müssen sich nicht mehr merken, wo sich Einstellungen in der Systemsteuerung befinden. Dies ist insbesondere dann hilfreich, wenn Sie Einstellungen schnell anpassen müssen, um Ihren mobilen PC an unterschiedlichen Orten zu verwenden, zum Beispiel auf dem Weg von Ihrem Schreibtisch in eine Besprechung oder auf dem Weg vom Flughafen nach Hause. Dadurch, dass Sie diese Einstellungen zentral anpassen können, sparen Sie Zeit, ganz gleich, ob Sie Ihren mobilen PC für geschäftliche oder private Zwecke verwenden.

Sie können das Mobilitätscenter mit einer der folgenden Methoden öffnen:

- Klicken Sie auf die Schaltfläche *Start*, klicken Sie auf *Systemsteuerung*, klicken Sie auf *Mobil-PC*, und klicken Sie dann auf *Windows-Mobilitätscenter*.
- Klicken Sie auf das Symbol für die *Akkumessanzeige* im Infobereich der Windows-Taskleiste, und klicken Sie dann auf *Windows-Mobilitätscenter*.
- Drücken Sie Windows-Logo-Taste + X.

Das Mobilitätscenter besteht aus mehreren der am häufigsten verwendeten mobilen PC-Einstellungen. Je nach System weist das Fenster des Mobilitätscenters einige, möglicherweise jedoch nicht alle der folgenden Kacheln auf:

- **Helligkeit**. Ziehen Sie den Schieberegler, um die Helligkeit der Anzeige vorübergehend anzupassen. Um die Helligkeitseinstellungen des Bildschirms für Ihren Energiesparplan anzupassen, klicken Sie auf das Symbol auf der Kachel, um Energieoptionen in der Systemsteuerung zu öffnen.
- **Lautstärke**. Ziehen Sie den Schieberegler, um die Lautsprecherlautstärke des mobilen PCs anzupassen, oder aktivieren Sie das Kontrollkästchen *Ton aus*.
- **Akkustatus**. Zeigen Sie die Restkapazität des Akkus an, oder wählen Sie aus einer Liste einen Energiesparplan aus.
- **Drahtlosnetzwerk**. Zeigen Sie den Status der Drahtlosnetzwerkverbindung an, oder schalten Sie den Drahtlosnetzwerkadapter ein oder aus.
- **Bildschirmausrichtung**. Ändern Sie die Ausrichtung des Bildschirms des Tablet PCs von Hochformat in Querformat und umgekehrt.
- **Externer Bildschirm**. Schließen Sie einen zusätzlichen Monitor am mobilen PC an, oder passen Sie die Anzeigeeinstellungen an.
- **Synchronisierungscenter**. Zeigen Sie den Status einer laufenden Dateisynchronisierung an, starten Sie eine neue Synchronisierung, und passen Sie die Einstellungen im Synchronisierungscenter an.
- **Präsentationseinstellungen**. Passen Sie Einstellungen wie die Lautsprecherlautstärke und das Desktophintergrundbild an, um eine Präsentation zu halten.

Wenn Sie weitere Anpassungen an den Einstellungen Ihres mobilen PCs vornehmen müssen, für die Sie auf die Systemsteuerung zugreifen müssen, klicken Sie auf das Symbol auf einer Kachel, um die Systemsteuerung für diese Einstellungen zu öffnen. Sie können beispielsweise einen vorhandenen Energiesparplan aus der Kachel Akkustatus auswählen, oder Sie können auf das Symbol auf der Kachel klicken, um zum Erstellen eines Energiesparplans Energieoptionen in der Systemsteuerung zu öffnen.

Hinweise

- Einige Kacheln im Mobilitätscenter wurden vom Hersteller Ihres mobilen PCs hinzugefügt. Weitere Informationen hierzu finden Sie in der Begleitdokumentation zu Ihrem mobilen PC oder auf der Website des Herstellers.
- Wenn eine Kachel nicht angezeigt wird, kann dies daran liegen, dass die erforderliche Hardware, z. B. ein Drahtlosnetzwerkadapter, oder die erforderlichen Treiber fehlen.

Synchronisierungscenter

In Windows bezeichnet Synchronisierung den Vorgang, Dateien an zwei oder mehr Orten identisch zu halten.

Die Synchronisierung kann unidirektional oder bidirektional erfolgen. Bei der unidirektionalen Synchronisierung werden jedes Mal, wenn Sie eine Datei oder andere Informationen an einem Ort hinzufügen, ändern oder löschen, dieselben Informationen am anderen Ort hinzugefügt, geändert oder gelöscht. Es werden jedoch nie Änderungen am ersten Ort ausgeführt, da die Synchronisierung nur in einer Richtung erfolgt.

Bei der bidirektionalen Synchronisierung werden Dateien in beide Richtungen kopiert, um die Dateien an beiden Orten synchron zu halten. Jedes Mal, wenn Sie eine Datei an einem Ort hinzufügen, ändern oder löschen, wird dieselbe Änderung am anderen Ort ausgeführt. Es spielt keine Rolle, ob Sie die Änderungen auf einem Computer, einem mobilen Gerät oder in einem Ordner auf einem Netzwerkserver vorgenommen haben. Dieselben Änderungen an beiden Orten ausgeführt. Die bidirektionale Synchronisierung wird meist in Arbeitsumgebungen verwendet, in denen Dateien häufig an mehreren Orten aktualisiert und dann mit anderen Orten synchronisiert werden.

Im Synchronisierungscenter können Sie den Computer mit Netzwerkordnern, mobilen Geräten und kompatiblen Programmen synchronisieren. Das Synchronisierungscenter kann Dateien und Ordner an verschiedenen Orten automatisch synchron halten.