

Musterlösung
für Schulen in
Baden-Württemberg

Windows 2000

Datensicherung

Musterlösung Windows 2000 / 2003

Autor: Detlef Schreiber

Inhaltsverzeichnis

Datensicherung	1
Musterlösung Windows 2000 / 2003	1
Autor: Detlef Schreiber	1
1 Sicherung von Netzwerkservern durch spezielle Hardware	3
1.1 Ausfallhäufigkeit verschiedener Hardwarekomponenten	3
1.2 Wissenswertes über RAID (Redundant Array of Independent Disks).....	4
1.2.1 RAID 0 - Data Striping.....	4
1.2.2 RAID 1 - Spiegeln (Disk Mirroring/Disk Duplexing)	5
1.2.3 RAID 4 - Data Striping mit separater Parity Festplatte	5
1.2.4 RAID 5 - Data Striping mit verteilter Parity.....	6
1.2.5 RAID 10 - Kombination aus RAID 1 und RAID 0	6
1.2.6 Chaining	7
1.2.7 Hot Plug	7
1.2.8 Hot Fix	7
1.2.9 SAF-TE (SCSI Accessed Fault - Tolerant Enclosure)	8
2 Datensicherung im Netzwerk.....	9
2.1 Serversicherung mit <i>Acronis True Image Server</i>	9
2.1.1 Neues Abbild erstellen	10
2.1.2 Automatisiertes Sichern mit Hilfe von Tasks.....	13
2.1.3 Wiederherstellung von Abbildern.....	16

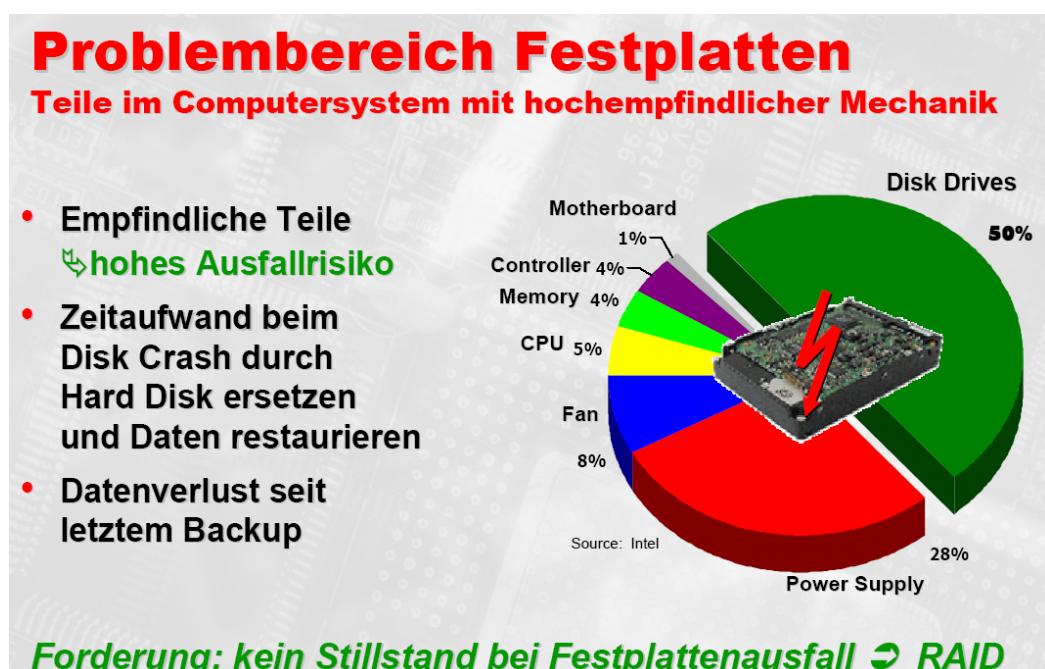
1 Sicherung von Netzwerkservern durch spezielle Hardware

Alle Teile eines Computersystems werden früher oder später durch technische Defekte den kompletten oder zumindest den teilweisen Ausfall der Anlage hervorrufen. Das muss nicht zwangsläufig zu Datenverlusten führen, je nachdem welche Systemkomponente diesen Ausfall verursacht. Die kritischsten Bauteile sind hierbei die Festplatten, da sich bei ihnen mechanische Bauteile mit hoher Geschwindigkeit und Genauigkeit bewegen und das meist über viele Jahre. Die auf den Festplatten gespeicherten Daten sind deshalb durch Hardwareausfälle besonders gefährdet.

In serverbasierten Computernetzen ist der Server hier besonders betroffen. Er soll jahrelang rund um die Uhr das Netz versorgen, das heißt alle Bauteile müssen für diese hohen Anforderungen ausgelegt werden. Trotzdem kann auch hier der Ausfall einzelner Komponenten nicht ausgeschlossen werden. Aus diesem Grund wird im Serverbereich versucht, durch redundante Bauweise die Sicherheit der gespeicherten Daten zu erhöhen.

Eine der wichtigsten Methoden um eine hohe Ausfallsicherheit im Serverbereich zu erreichen ist der Einsatz von RAID-Systemen. Diese werden in der Folge vorgestellt. Sie werden in der Regel aus dauerbetriebsfesten **SCSI-Festplatten** bestehen, sind heute aber auch schon mit kostengünstigeren, servertauglichen IDE- oder SATA-Festplatten erhältlich.

1.1 Ausfallhäufigkeit verschiedener Hardwarekomponenten



1.2 Wissenswertes über RAID (Redundant Array of Independent Disks)

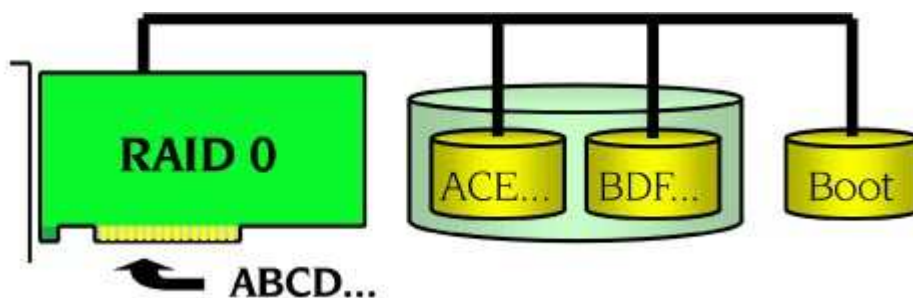
Die RAID Technologie hat heute ihren festen Platz im Bereich der Server-Systeme und high performance Workstations. Kunden die solche Systeme konfigurieren und einsetzen erwarten von dem Disk-Array System:

- Hohe Leistung
- Hohe Kapazität
- Fehlertoleranz
- Zuverlässigkeit
- Adequater Preis
- Einfache Bedienungs- und Wartungsmöglichkeiten

Der Disk Array Controller und die angeschlossenen Festplatten werden als integraler und wichtiger Bestandteil des Gesamtsystems identifiziert. State-of-the-Art Produkte erfüllen und maximieren alle diese Anforderungen gleichermaßen. Das erfolgreiche Design und die effiziente Entwicklung von Disk Array Controllern fordern nicht nur sehr viel Know-how, sondern auch ein großes Erfahrungsspektrum.

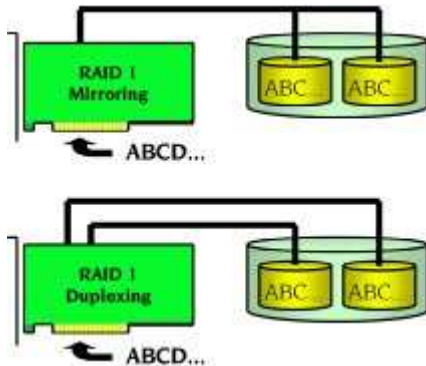
Wer sich heute mit RAID befasst, setzt sich zwangsläufig mit den unterschiedlichen RAID-Levels auseinander. Nachfolgend finden Sie eine Auflistung der am häufigsten eingesetzten RAID-Levels:

1.2.1 RAID 0 - Data Striping



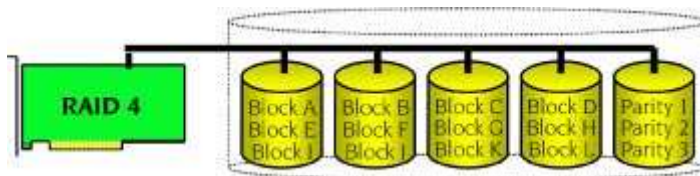
Die Datenblöcke werden entsprechend der eingestellten Streifengröße (z.B. 16KB) und der vorhandenen Festplatten in Streifen (eng. stripes) aufgeteilt, wobei jeder Streifen eines Datenblocks auf einer separaten Festplatte gespeichert wird. Dadurch wird vor allem beim sequentiellen Schreiben und Lesen von großen Dateien ein deutlich höherer Datendurchsatz erreicht. RAID 0 bietet keinerlei Redundanz. Beim Ausfall einer Festplatte sind die Daten des gesamten RAID 0 Verbandes verloren.

1.2.2 RAID 1 - Spiegeln (Disk Mirroring/Disk Duplexing)



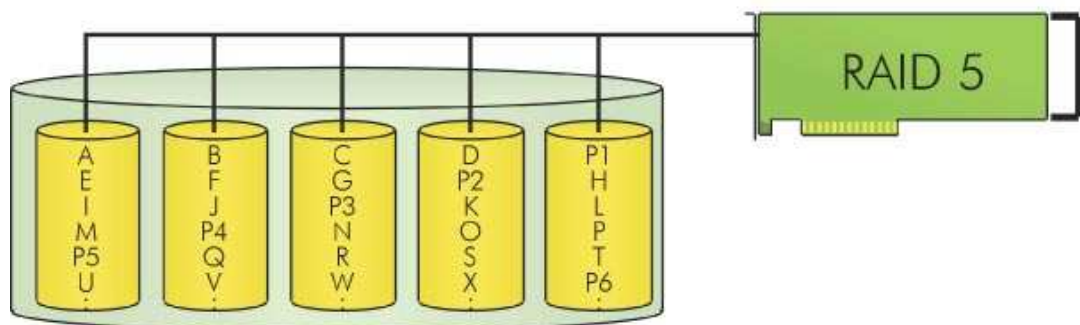
Die Daten werden jeweils auf zwei Festplatten gespeichert. Beim Ausfall einer Platte sind die Daten identisch auf der zweiten Festplatte vorhanden. Beim Spiegeln von Festplatten an einem Kanal spricht man von Disk Mirroring, beim Spiegeln an unabhängigen Kanälen von Disk Duplexing (zusätzliche Sicherheit). RAID 1 ist eine einfache und schnelle Lösung zur Datensicherheit und Datenverfügbarkeit, besonders geeignet für kleinere Nutzkapazitäten. Lediglich die Hälfte der Gesamtkapazität steht als nutzbarer Bereich zur Verfügung.

1.2.3 RAID 4 - Data Striping mit separater Parity Festplatte



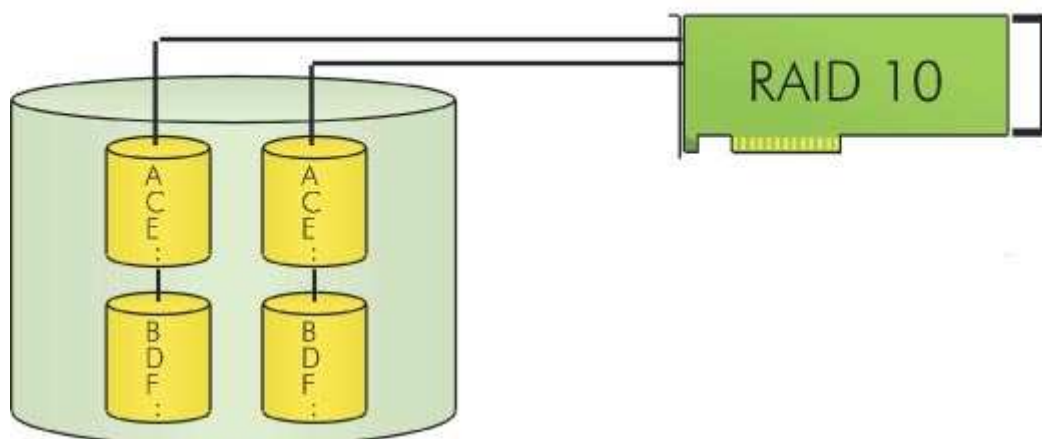
Wie bei RAID 0 werden die Daten auf den Festplatten verteilt. Auf einem Sicherheitslaufwerk werden Paritätsdaten abgelegt. Durch diese Parität stehen selbst bei einem Ausfall einer Festplatte alle Daten weiterhin zur Verfügung. Lediglich die Kapazität einer Festplatte geht für die Redundanz verloren. Bei einem RAID 4 Verband mit 5 Festplatten stehen 80 Prozent der Gesamtkapazität als Nutzkapazität zur Verfügung. Beim Schreiben kleiner Datenblöcke wird das Paritylaufwerk sehr stark belastet was die Performance deutlich negativ beeinflusst. RAID 4 bringt vor allem beim Schreiben und Lesen großer Dateien eine optimale Performance.

1.2.4 RAID 5 - Data Striping mit verteilter Parity



Anders als bei RAID 4 werden die Paritätsdaten auf allen Festplatten im Verband gleichmäßig verteilt. Dies garantiert bei allen Zugriffen eine optimale Auslastung der Laufwerke. Selbst bei kleinen random Zugriffen, wie sie für ein multitasking multiuser Betriebssystem typisch sind, kann somit eine optimale Performance erreicht werden. RAID 5 bietet gleiche Sicherheit wie RAID 4 - Datenverfügbarkeit beim Ausfall einer Festplatte. RAID 4 und RAID 5 sind vor allem für Systeme mit mittleren und großen Nutzkapazitäten geeignet. Hier macht sich besonders das wirtschaftliche Verhältnis zwischen Gesamt- und Nutzkapazität positiv bemerkbar.

1.2.5 RAID 10 - Kombination aus RAID 1 und RAID 0



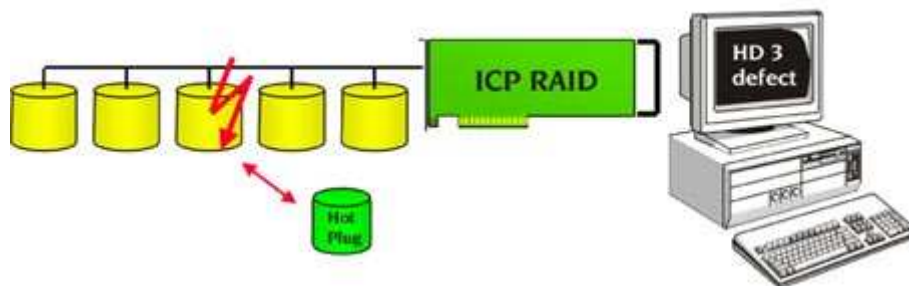
Aus einer Kombination zwischen RAID 0 (Performance) und RAID 1 (Datensicherheit) ist der RAID Level 10 entstanden. RAID 10 Verbände bieten optimale Performance bei optimaler Ausfallsicherheit. Wie bei RAID 0 wird die optimale Geschwindigkeit allerdings nur bei sequentiellen Zugriffen erreicht und wie bei RAID 1 gehen 50 Prozent der Gesamtkapazität für die Redundanz verloren. RAID 10 ist für Systeme kleinerer Nutzkapazität geeignet bei denen optimaler Datendurchsatz mit optimaler Datensicherheit verknüpft werden soll.

1.2.6 Chaining

Aneinanderreihung ("Kette" engl. chain) von mehreren Festplatten zu einem großen logischen Laufwerk. Die einzelnen festplatten werden sozusagen nacheinander mit Daten "gefüllt". Fällt eine Festplatte aus fehlen alle Daten, die sich auf diesem Laufwerk befunden haben. D. h. es existiert keinerlei Redundanz.

1.2.7 Hot Plug

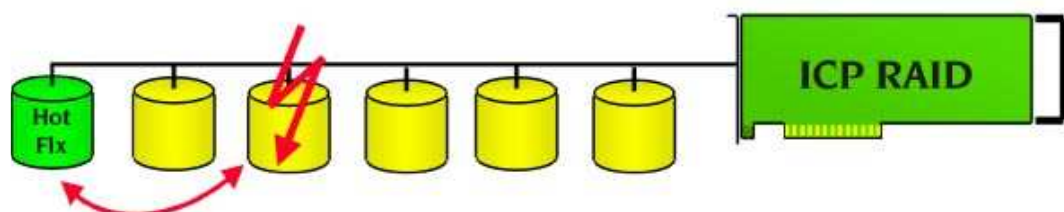
Austausch einer defekten Festplatte eines RAID Verbandes im Betrieb (oftmals auch als Hot Swap bezeichnet).



- Beim Hot Plug wird die Ersatzfestplatte im Betrieb manuell getauscht
- Während Hot Plug besteht weiterhin volle Datenverfügbarkeit
- Hot Plug im ICPCON integriert und unter jedem unterstütztem Betriebssystem verfügbar
- Einbindung der Ersatzfestplatte geschieht automatisch durch das Hot Plug Programm

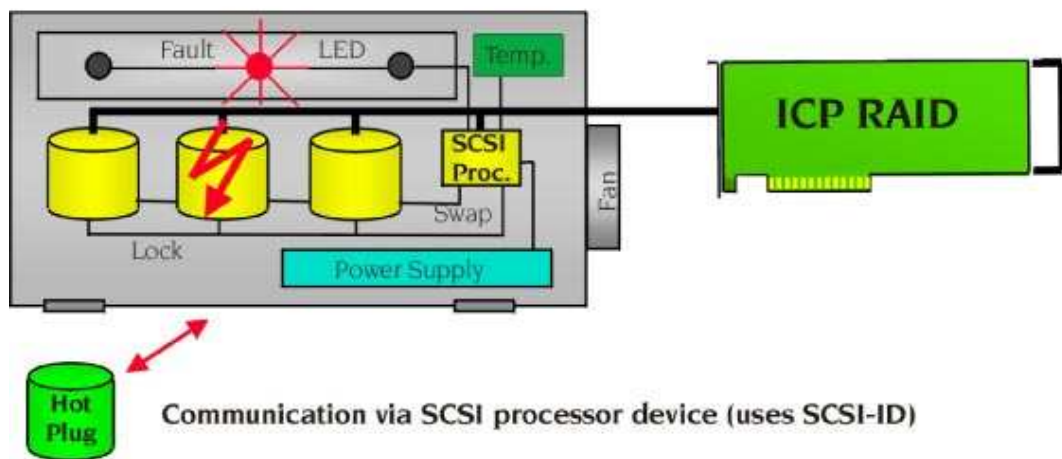
1.2.8 Hot Fix

Automatischer Ersatz einer defekten Festplatte in einem RAID Verband durch ein so genanntes Hot Fix Laufwerk (oftmals auch Stand-By Laufwerk genannt).



- bereits eingebaute, nicht aktive Ersatzfestplatte
- Hot Fix Laufwerke werden zyklisch auf Funktion überprüft
- Festplattenausfall aktiviert Hot Fix und ersetzt defekte Festplatte
- Private Hot Fix: nur für einen RAID Verband verfügbar
- Pool Hot Fix: ein oder mehrere Hot Fix Laufwerke für einen oder mehrere RAID Verbände verfügbar

1.2.9 SAF-TE (SCSI Accessed Fault - Tolerant Enclosure)



- SAF-TE Device kommuniziert mit dem Controller wie jedes andere SCSI Gerät (benötigt freie SCSI-ID)
- Status LED: Anzeige von Laufwerkszuständen (z.B.: ready, fail, rebuild, usw.)
- Auto Hot Plug: Hot Plug lediglich durch Austausch der Festplatte ohne User Interaktion (ICPCON)
- Shelf Management: Überwachung von Temperatur, Lüfter, Netzteile, Einschübe, usw.

2 Datensicherung im Netzwerk

Zur Sicherung von Programminstallationen und Benutzerdaten in Netzwerken setzen größere Firmen und Verwaltungen Datenbänder ein. Diese Bänder müssen dann zum jeweils gewünschten Zeitpunkt ausgetauscht und sicher verwahrt werden.

Abgesehen davon, dass diese so genannten Streamer, die dazugehörigen Bänder und die notwendige Sicherungssoftware keine ganz billige Methode der Datensicherung darstellen, so sind sie auch deshalb etwas unpraktisch, weil der Netzwerkberater / Systembetreuer jedes Mal den Server aufsuchen muss, wenn eine neue Sicherung notwendig wird.

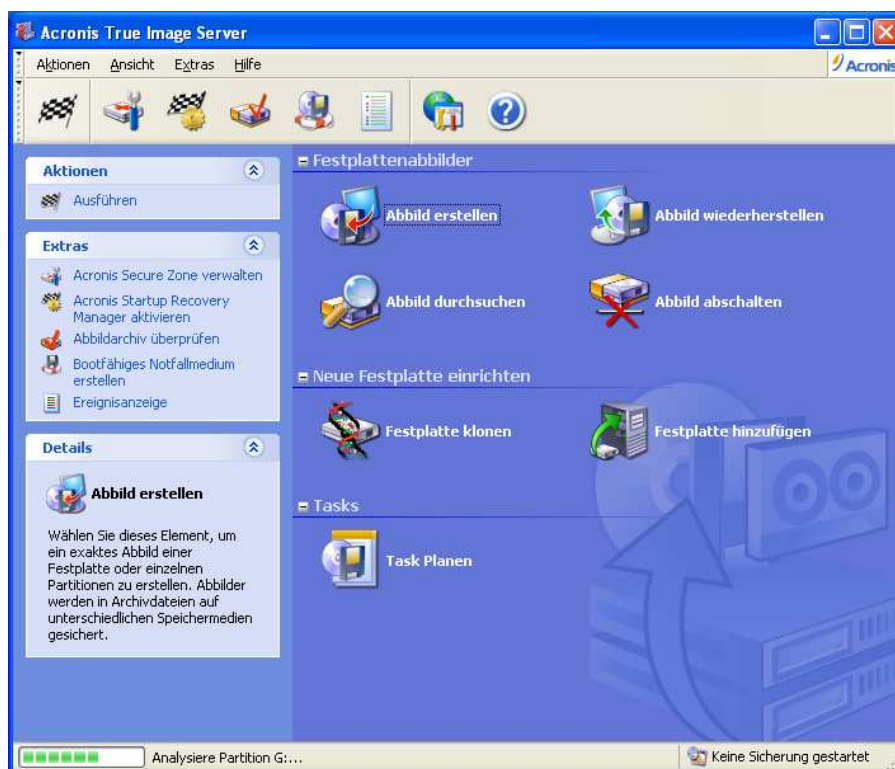
In vielen Fällen kann man im schulischen Bereich auf kostengünstigere und vielleicht auch noch etwas weniger aufwendige Art die notwendigen Sicherungen durchführen.

Neben den schon seit langem bekannten Imaging-Tools von **Symantec** oder **Powerquest**, bietet auch die Firma **ACRONIS** eine servertaugliche Sicherungssoftware an. Diese wird für die allgemeinbildenden und beruflichen Schulen zu einem stark reduzierten Preis angeboten. Von ihr wird in der Folge die Rede sein.

Besonders ideal sind die neueren Tools deswegen, da sie die Sicherung des Servers im laufenden Betrieb ermöglichen und auf alle vorhandenen Laufwerke sichern können. Im Zusammenspiel mit einer externen USB- oder Firewire – Festplatte können so auch große Datenmengen zeitgesteuert und ohne manuellen Eingriff gesichert werden. Da externe Festplatten sich in aller Regel nach einiger Zeit selbst in den Ruhezustand begeben (d.h. sie schalten den Spindelmotor ab), wird ihr Verschleiß auf ein Minimum reduziert.

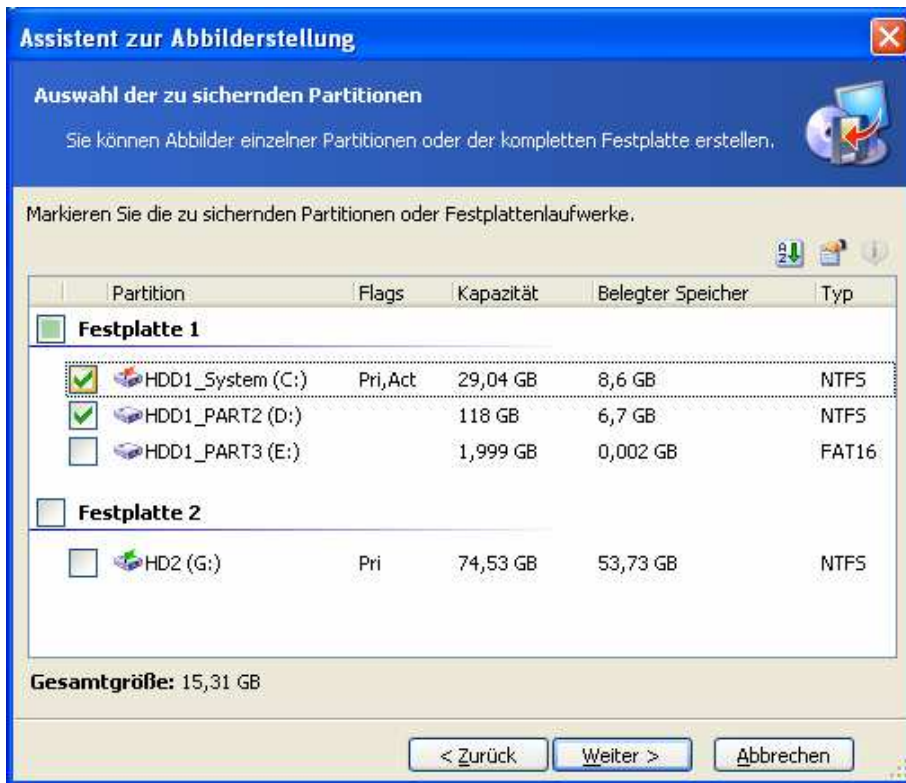
Eine Sicherheit gegen Diebstahl, Feuer, Wasser oder sonstige Naturkatastrophen erreicht man allerdings nur, wenn das gesicherte Medium danach in einem entsprechenden Safe aufbewahrt wird!

2.1 Serversicherung mit *Acronis True Image Server*

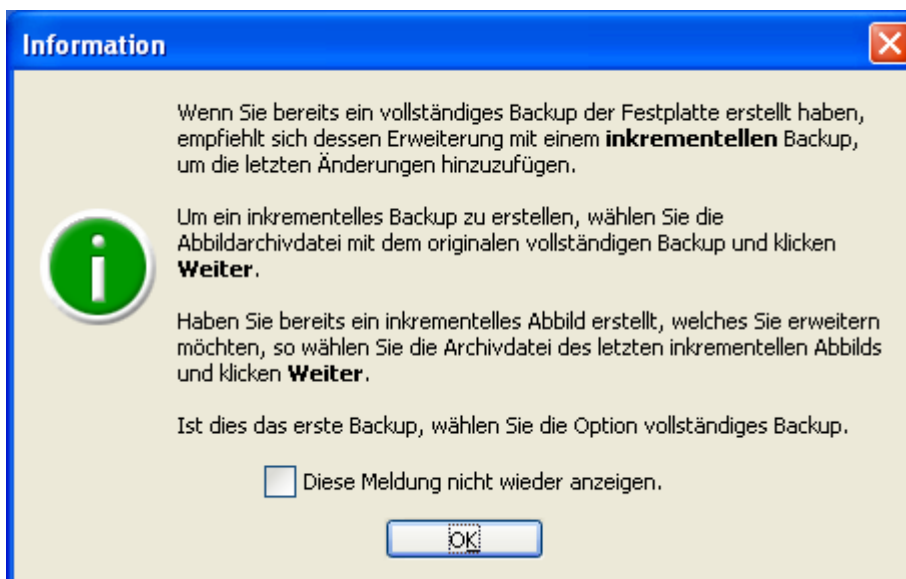


2.1.1 Neues Abbild erstellen

Die zu sichernde Festplatte oder einzelne Partitionen werden ausgewählt



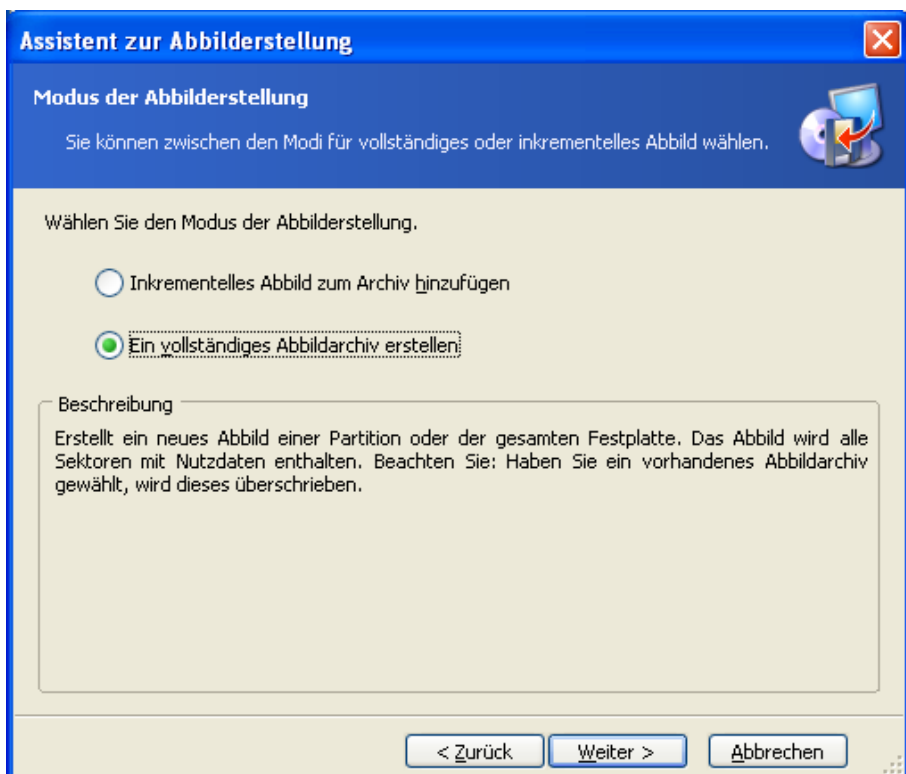
Liegt bereits ein älteres Abbild der Festplatte vor, so kann auch eine inkrementelle Sicherung durchgeführt werden, d.h. nur die Veränderungen der Installation seit der letzten Sicherung werden gespeichert. Das spart Speicherplatz, da sich dadurch die Größe der neuen Sicherungsdatei erheblich reduziert.



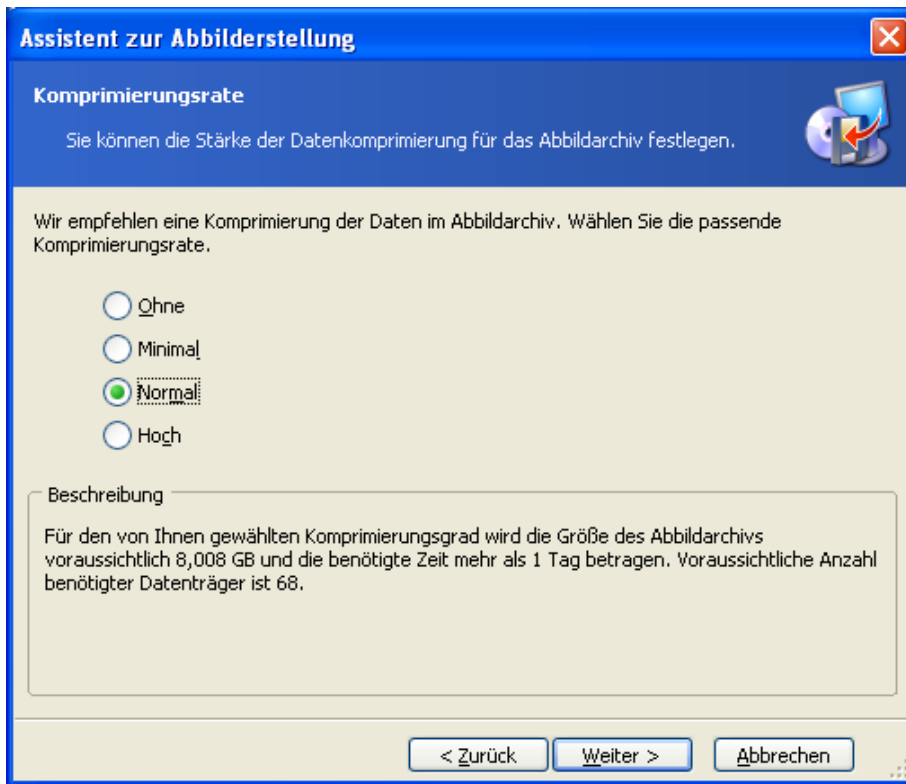
Nun wählt man den Speicherort und den Namen der neuen Backupdatei aus. Dabei sind alle angezeigten Laufwerke, auch die Netzlaufwerke, als Speichermedien denkbar. CD- und DVD- Brenner machen da keine Ausnahme, sie kommen wegen ihres begrenzten Speichervolumens aber weniger in Frage. Externe USB2.0- Speichermedien (Festplatten) sind kostengünstig, schnell und damit unsere erste Wahl.



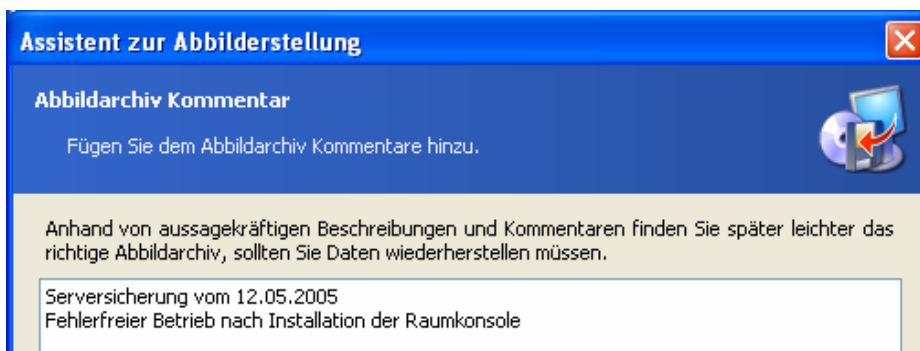
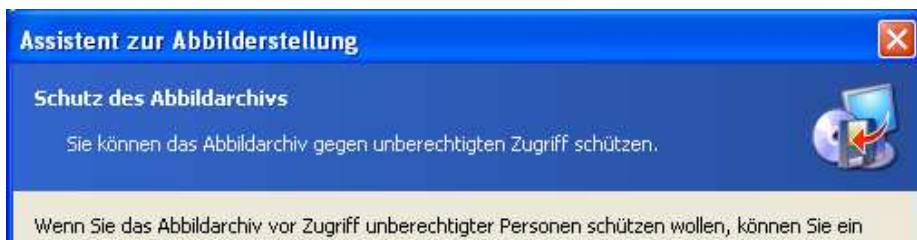
Nun entscheidet man sich für ein neues, vollständiges Abbild oder, wenn kann ein inkrementelles Abbild zu einer bereits bestehenden Sicherungsdatei hinzufügen.



True Image bietet nun die Möglichkeit an, manuell eine Komprimierungsstufe zu wählen, wobei „**Normal**“ eine recht gute Komprimierung bei hoher Geschwindigkeit bietet. Sollte der Datenträger sehr klein (wie im Beispiel) und die Datenübertragungsrage gering sein, so kann man das ebenfalls in diesem Fenster ablesen.



Neben der Möglichkeit, das Abbild durch ein Passwort zu schützen, bietet *True Image Server* dann die Möglichkeit an, einen aussagekräftigen Kommentar zu Abbild hinzuzufügen, der später eine Unterscheidung der verschiedenen Sicherungsdateien erleichtert.

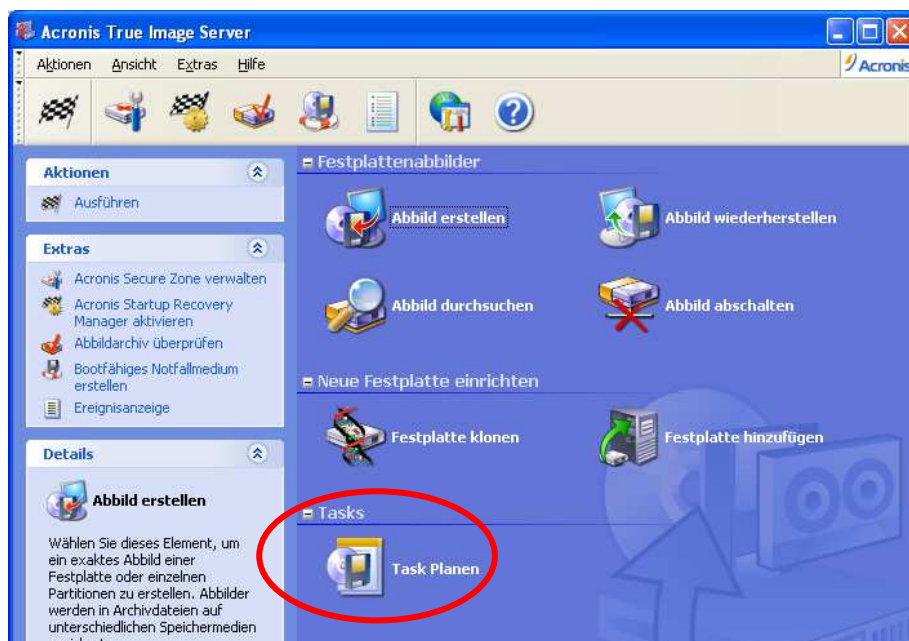


Das letzte Fenster zeigt noch einmal eine Zusammenfassung aller gewählten Einstellungen. Danach startet man über die Schaltfläche „Fertig stellen“ die Erstellung des Abbilds.



2.1.2 Automatisiertes Sichern mit Hilfe von Tasks

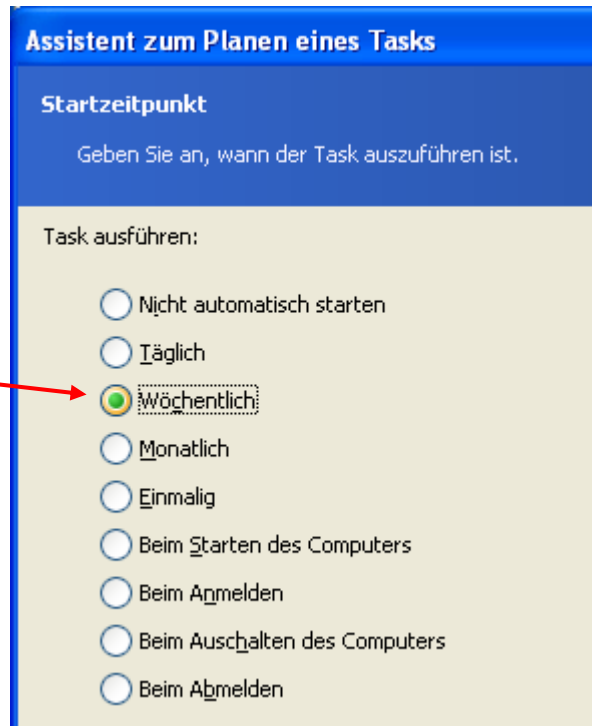
True Image Server bietet auch die Möglichkeit, den Sicherungsprozess automatisiert zu einem festgelegten Zeitpunkt zu starten. Das hat den Vorteil, dass die Serversicherung in die Nachtstunden oder auf das Wochenende verlegt werden kann, wenn vermutlich keine Benutzerzugriffe erfolgen. Damit steht die gesamte Rechenleistung des Prozessors allein für den Sicherungsprozess zur Verfügung.



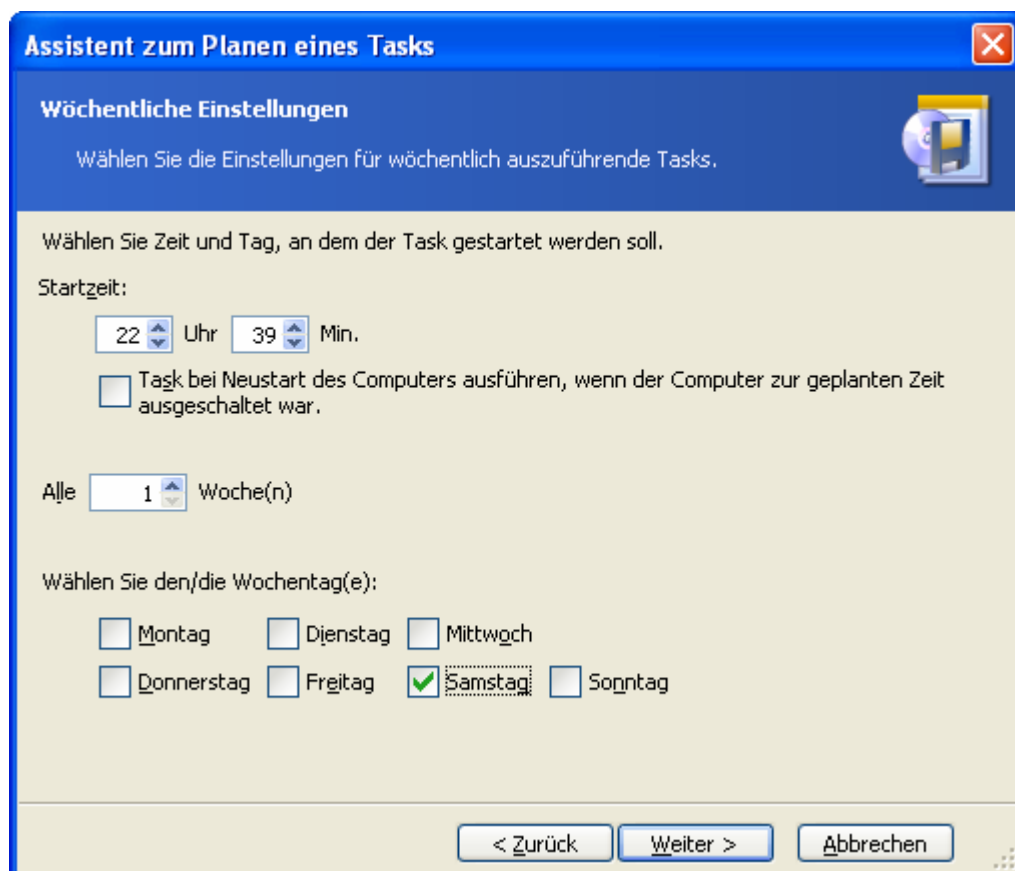
Bis zum vorletzten Schritt des unter **2.1.1** beschriebenen Vorgangs ist die Vorgehensweise bei der Erstellung eines Tasks nahezu identisch.

Neu ist jetzt allerdings die Auswahlmöglichkeit für den Startzeitpunkt des Sicherungsprozesses.

Eine wöchentliche Sicherung könnte fürs erste genügen. Sollten sich die Benutzerdaten aber schnell ändern, so käme auch eine tägliche Sicherung in Betracht.



Im nächsten Fenster legt man die Uhrzeit und den Wochentag fest. Man kann hier den Zyklus auch auf mehrere Wochen verlängern oder festlegen, ob eine Sicherung beim Neustart erfolgen soll, falls der Server beim vorgesehenen Zeitpunkt abgeschaltet war.



Nach der Eingabe des Benutzernamens (am Server mit Domänenbezeichnung) und eines gültigen Passworts erscheint noch einmal eine Zusammenfassung aller bereits festgelegten Daten, bevor über „Fertigstellen“ der Task abgeschlossen wird.

Assistent zum Planen eines Tasks

Benutzerinformation

Geben Sie Benutzernamen und Kennwort an.

Geben Sie den Namen und das Kennwort eines Benutzers ein. Der Task wird so ausgeführt, als ob er von diesem Benutzer gestartet wurde. Vergessen Sie nicht den Domännennamen anzugeben, falls der Benutzer Mitglied einer Domäne ist

Geben Sie den Benutzernamen ein:

Geben Sie das Kennwort des Benutzers ein:

Kennwort bestätigen:

Wenn Sie kein Kennwort eingeben, kann der Task möglicherweise nicht ausgeführt werden.

< Zurück Weiter > Abbrechen

Assistent zum Planen eines Tasks

Acronis True Image Server

Acronis True Image kann nun mit der Erstellung des neuen Tasks beginnen.

Zusammenfassung der Aktion:
Vollständiges Abbild erstellen
 Von: HDD1_PART2 (D:) HDD1_System (C:),
 In Datei: "P:\MeinBackup.tib"
 Komprimierung: Normal

Geplant:
Um 23:43:00 jede Woche am Samstag

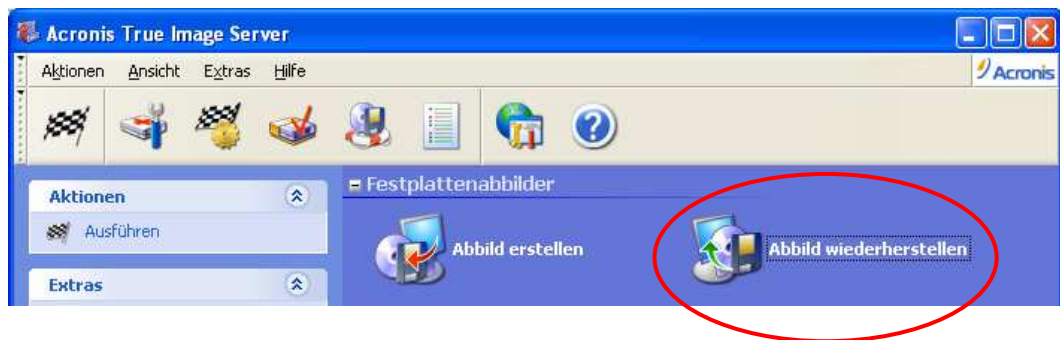
Aktion 1 von 2
Partitionsabbild erstellen
 Festplatte: 1
 Laufwerksbuchstabe: C:
 Dateisystem: NTFS
 Datenträgerbezeichnung: HDD1_System
 Größe: 29,04 GB

Aktion 2 von 2
Partitionsabbild erstellen
 Festplatte: 1

Drücken Sie **Fertig stellen**, um den Vorgang abzuschließen.

< Zurück Fertig stellen Abbrechen

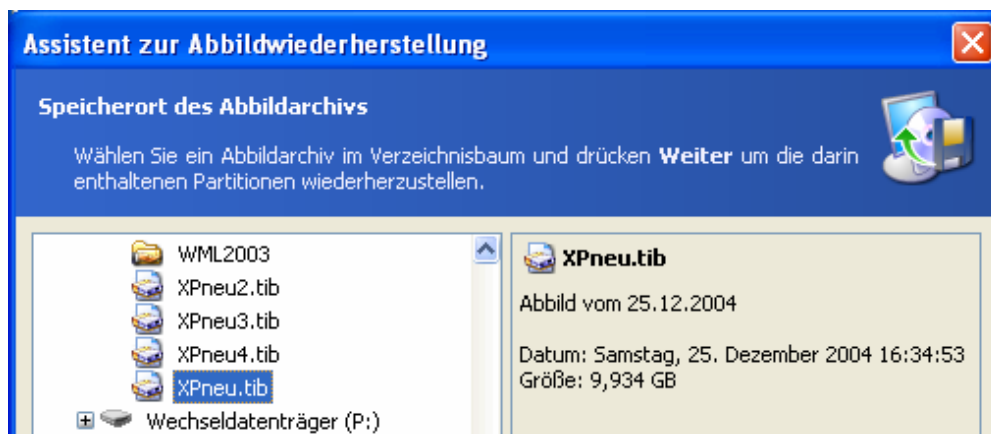
2.1.3 Wiederherstellung von Abbildern



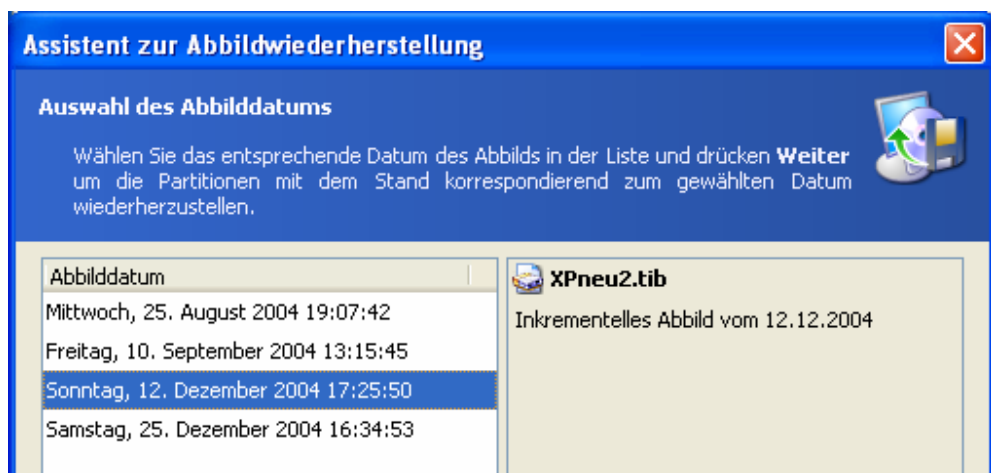
Die Erstellung von Abbildern mit Hilfe einer Sicherungssoftware wie beispielsweise True Image macht nur dann Sinn, wenn zuvor geklärt wurde, ob das System bei einem Totalausfall mit Hilfe eines Notfallmediums wieder gestartet werden kann.

Obwohl sich die Firmen alle Mühe geben, so liegen Ihnen zum Zeitpunkt der Programmerstellung sicherlich nie alle Treiberdateien für die auf dem Markt erhältlichen Controller vor. Es muss deshalb Aufgabe des Händlers sein, der den Server liefert, dafür zu sorgen, dass ein solches Notfallmedium mit entsprechender Treiberausstattung vorliegt.

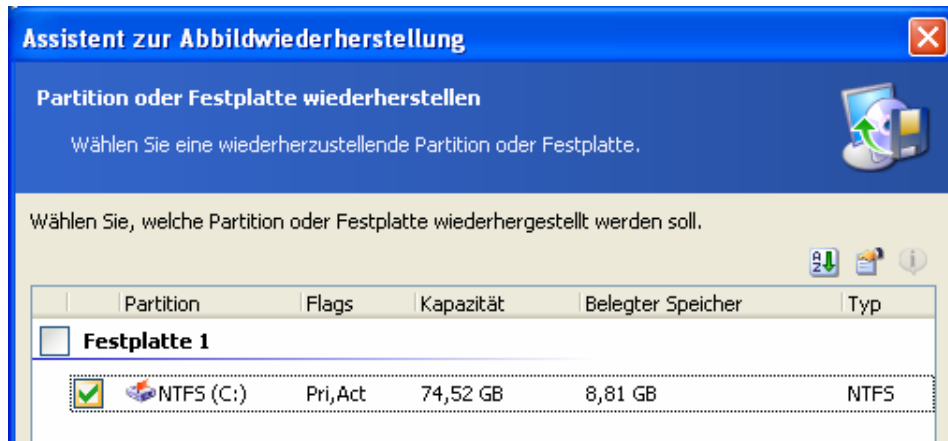
Nach dem Start des Assistenten wählt man die passende Abbilddatei. Dabei kann der erläuternde Text im rechten Fenster hilfreich sein.



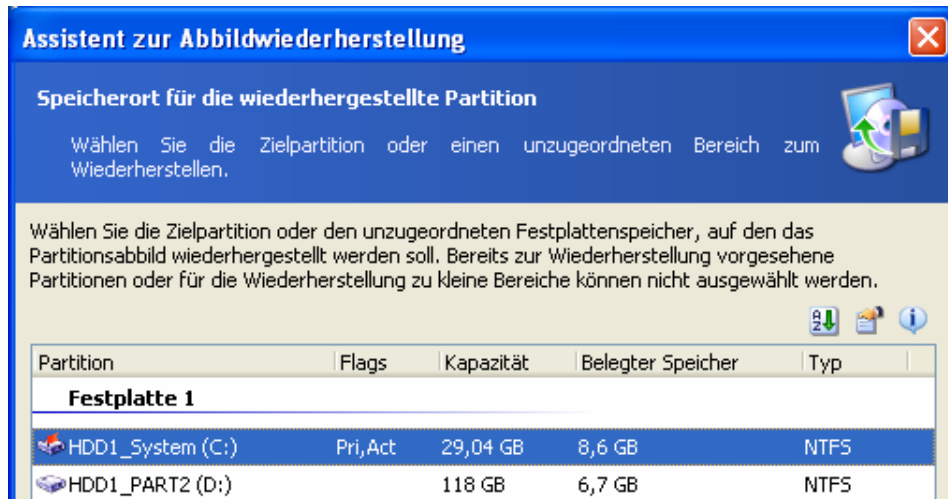
Im nächsten Fenster werden, falls vorhanden, dazu passende, inkrementelle Abbilder angezeigt.



Wählen Sie die im Abbild enthaltenen Festplatte- oder Partitionsdaten, die Sie wiederherstellen möchten.



Das Speicherziel kann dann jede beliebige Platte sein, die genügend Platz bietet, um die Daten aus der Abbilddatei aufnehmen zu können.



Sollte es sich bei der wiederherzustellenden Partition um den Systembereich handeln, so empfiehlt es sich, die Wiederherstellung im abgesicherten Modus während eines Neustarts vorzunehmen.

