Projekt Backup- und Recovery-Prozesse

Backups - Die letzte Rettung

Virenbefall, Festplattendefekt, Programmfehler oder Unachtsamkeit: Daten sind ständig in Gefahr. Wohl dem, der im Ernstfall über ein aktuelles Festplattenimage verfügt. Dennoch wird gerade das Thema Backup noch immer von vielen PC-Besitzern eher vernachlässigt.

Die effiziente Sicherung und Wiederherstellung von Daten stellt Unternehmen aller Größenordnungen seit Jahrzehnten vor immer neue Herausforderungen. Lange Zeit betrachteten Administratoren Backup-Vorgänge als notwendiges Übel, das in der Regel nur sehr langsam voran geht, mit viel Aufwand verbunden ist und dessen Verlässlichkeit in vielen Fällen zu wünschen übrig lässt. Auch unter Kostengesichtspunkten war der Bereich Backup und Recovery lange einsame Spitze innerhalb der IT: Nahezu zwei Drittel aller Aufwendungen für Speicher-Management entstehen laut einer Studie der META Group durch fehlgeschlagene Backup-Prozesse, ausgefallene Bandlaufwerke oder Medienfehler.

Die zunehmende Datenflut in den Unternehmen und strengegesetzliche Regelungen zur revisionssicheren Archivierung und Sicherung von Daten tun ein Übriges. Sie zwingen dieVerantwortlichen, ihre Backup-Strategien zu überdenken und neu aufzusetzen. Neue Technologien und Software-Lösungen unterstützen sie dabei, ein verlässliches, effizientes Backup einzuführen, das den geschäftlichen Anforderungen und gesetzlichen Richtlinien entspricht.

Allein die immens steigenden Informationsmengen in den Rechenzentren zwingen die Administratoren dazu, neue Verfahren und Strategien beim Backup zu implementieren. Marktforscher rechnen mit einem durchschnittlichen Datenwachstum von 50 Prozent und mehr. Die Datensicherung dauert folglich immer länger. Gleichzeitig werden in vielen Unternehmen die zur Verfügung stehenden Backup-Fenster reduziert, um wertvolle Netzwerk-Bandbreiten für andere Geschäftsprozesse nutzen zu können. Ähnlich strenge Vorgaben gelten für die Wiederherstellung im Falle eines Datenverlusts oder Ausfalls der Produktivsysteme. Viele Unternehmen fordern von ihren IT-Verantwortlichen die Garantie, verlorene Informationen nach einem Ausfall innerhalb von Minuten wiederherstellen zu können anstelle Seite 2 von 5von Stunden oder gar Tagen. Diese Anforderungen und Service Levels einzuhalten, wird für die IT-Abteilungen und Administratoren zunehmend schwierig.

Konkurrenzdruck und die Anforderungen einer dank Internet global operierenden Geschäftswelt zwingen die Unternehmen dazu, über eine Business-Continuance-Strategie nachzudenken, die eine Geschäftstätigkeit möglichst rund um die Uhr erlaubt. Kein international tätiges Unternehmen kann sich längere Ausfälle der IT oder gar Datenverluste leisten – noch dazu in Zeiten, in denen die Anforderungen des Gesetzgebers hinsichtlich Aufbewahrung und Löschung der unterschiedlichen Klassen von Informationen immer umfassender werden. Daher spielen Datensicherung und -wiederherstellung eine zentrale Rolle. Hinzu kommt häufig die neue Vorgabe, die Geschäftsprozesse effizienter zu gestalten. In vielen Unternehmen wird jeder einzelne Geschäfts- und IT-Prozess unter die Lupe genommen mit dem Ziel, diesen zu beschleunigen und die Kosten zu senken. Backup und Recovery stehen dabei oft an erster Stelle, denn Analysten zufolge verbringen IT-Abteilungen drei Viertel ihrer Zeit mit der Sicherung und Wiederherstellung von Daten. Dies bekräftigt *Anders Lofgren* von Forrester Research: „75 Prozent des Storage Managements sind Backup und Recovery, wobei 30 Prozent aller Recovery-Operationen fehlschlagen, weil das entsprechende Backup vermasselt wurde.“

Die Storage-Branche reagiert mit neuen Technologien und Strategien auf diese Herausforderungen und unterstützt Unternehmen dabei, ihre Daten verlässlich zu sichern und innerhalb kürzester Zeit wieder herzustellen.

Im folgenden Skript findet man allgemeine Ratschläge zu **Backupmedien** und **Backupstrategien** und lernt danach mehrere Sicherungsmöglichkeiten mittels Bordmitteln oder externer Share- und Freeware kennen. Zum Schluss beschäftigten wir uns dann noch mit der Problematik der **Systemsicherung** mittels **Image-Programmen** und der Trennung von Daten und System auf eigene Partitionen mit Hilfe von Programmen.

Allgemeines

Daten sind auf der Festplatte ständig in Gefahr! Eine defekte Festplatte kann ebenso zum Datenverlust führen wie Virenbefall, eine abgestützte Applikation oder auch nur unachtsames Löschen. Eine weitere Fehlerquelle für defekte Dateien ist das versehentliche Überschreiben durch eine ältere oder fehlerhafte Version eines Dokumentes.

Ohne Backup sieht es in allen Fällen für den Anwender schlecht aus.

Um diesen Fehlerquellen vorzubeugen, sollte man ein Backup der Daten haben. Ein Backup beinhaltet Kopien der gesicherten Dateien. Je nach verwendeter Software werden die Daten dabei in eine Backupdatei oder im Original gesichert. Auf diese Problematik gehen wir später noch ein.

Einen Sonderfall stellt die Sicherung des Systems und/oder der Daten mit einem Image-Programm wie *TrueImage* dar.

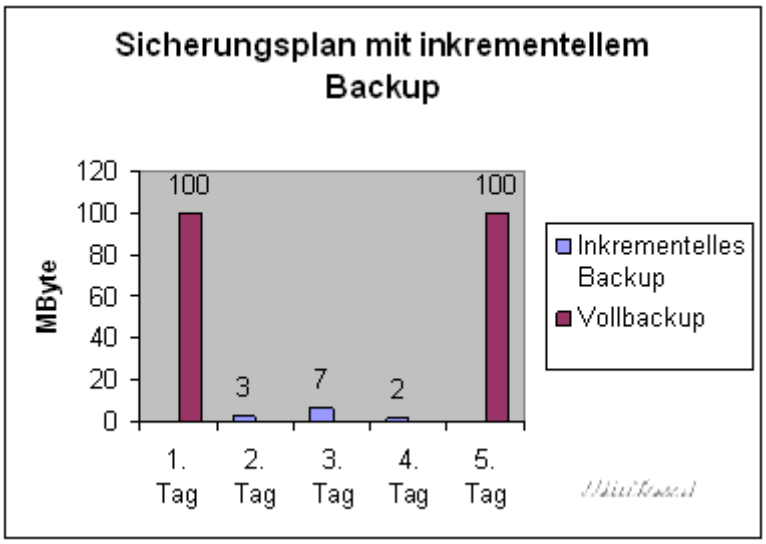
Wer Dateien auf die gleiche Festplatte sichert, macht eigentlich kein Backup, da bei einem Festplattendefekt oder Virus diese Daten im Regelfall ebenfalls betroffen sind. Der einzige und sicherste Weg ist daher die Sicherung aller relevanten Daten auf einem externen Speichermedium, welches nach der Sicherung nicht mehr mit dem System verbunden ist.

Backuparten

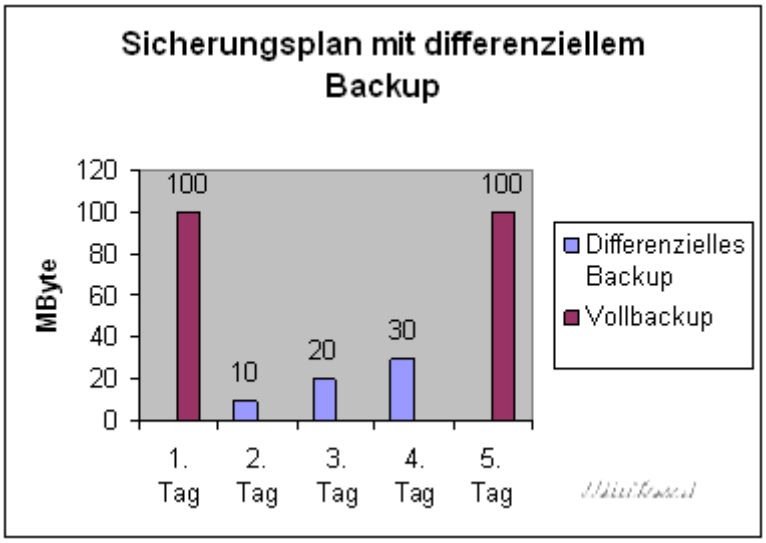
Man unterscheidet 3 verschiedene Backuparten:

- ✓ **Vollbackup**
  Hier werden alle selektierten Dateien gesichert.

- ✓ **Inkrementelles Backup**
  Diese Backupart sichert nur die Dateien, welche seit der letzten Sicherung neu hinzugekommen sind oder geändert wurden.
  Für eine Rücksicherung der Daten benötigt man daher das Vollbackup sowie alle inkrementellen Backups bis zum Tage des Ausfalls.



✓ **Differenzielles Backup**
Diese Backupart sichert alle Dateien, welche seit dem letzten Vollbackup geändert wurden oder neu hinzugekommen sind.
Für eine Rücksicherung benötigt man das Vollbackup sowie das letzte differenzielle Backup.



Für den Laien ergibt sich bei erster Betrachtung zwischen dem inkrementellen Backup und dem differenziellen Backup zunächst kein Unterschied.

Da bei der inkrementellen Sicherung aber nur die Veränderungen seit der letzten Sicherung gespeichert werden, sind diese Sicherungssätze im Vergleich zu einem differenziellen Backup wesentlich kleiner (siehe jeweils Werteangabe der Tage 2 bis 4 in den Diagrammen). Der Grund für diese Tatsache liegt darin, dass ein inkrementelles Backup nur die geänderten und neuen Daten seit der letzten Sicherung - dies kann ein Vollbackup oder ein inkrementelles Backup sein - speichert. Bei dem differenziellen Backup werden dagegen alle Daten seit dem letzten Vollbackup gesichert, egal wie viele "Zwischensicherungen" bisher erfolgt sind.

Daher benötigt man beim Zurücksichern mit inkrementellen Datensätzen neben dem Vollbackup alle danach noch anlegten inkrementellen Sicherungssätze. Die kleinere Speichergröße erkauft man sich daher mit mehr Verwaltungsaufwand (und damit mehr Fehlerquellen).

Für Anfänger und den "Heimgebrauch" kann ich aus eigener Erfahrung nur empfehlen, die Sicherungsmethoden einfach zu gestalten. Wer erst lange überlegen muss, welche Daten wann und wie oft bzw. wie gesichert werden, kommt im Schreckensfall - bedingt durch die Hektik - schnell ins Schleudern und spielt vielleicht die falschen Daten zurück.

Zudem sollte man sich mit dem eventuellen Notfall vertraut machen und die Rücksicherung der Daten ohne Erstfall simulieren. Besser man erkennt eventuelle Probleme vorab und kann diese beheben, als bei einem Rücksichern vor den Problemen zu stehen.

Backup im Original oder eigenen Dateiformat

Kopiert der Anwender Dateien auf ein anderes Speichermedium, sichert er diese im Original, d.h. Word-Dokumente, MP3, Bilder etc. Um Speicherplatz zu sparen, können diese Dateien auch in einem gängigen Dateiformat gepackt werden.

Viele Backupprogramme, aber auch Windows-Backup selbst, sichern die Daten dagegen in eigenen Dateiformaten, die untereinander nicht kompatibel sind. Selbst *Windows-Backup* nutzt in der Windows 98-Version ein anderes Dateiformat als der XP-Bruder. Die Programme speichern das gesamte Backup in eine einzige Datei (oft mit Kompression), welche die eigentlichen Daten und im Regelfall auch den Ursprung der Datei beinhaltet.

Ein Nachteil des eigenen Dateiformats ist die fehlende Verfügbarkeit des Backups ohne die eigentliche Software. Nur wenn diese Software installiert ist, kann man auch auf die Daten im Backup zugreifen. Wenn das System nicht mehr lauffähig ist, kommt man daher auch nicht an seine Backups heran. Vorteil dieser Methode ist der Schutz aller Daten im Backup vor Viren oder dem System selbst.

Sichert das Backupprogramm die Daten im Original, kann man im Regelfall mit allen anderen Systemen auf die Dateien wieder zugreifen.

Wann und wie oft ?

Am besten wäre immer und stündlich! Die Sicherungsintervalle hängen direkt mit dem Grad der Sicherheit zusammen, bei einem Ausfall die aktuellen Daten zu haben. Weitere Faktoren sind aber auch die Menge der zu sichernden Daten und das Backupmedium. Wer täglich 10 GByte an Daten auf einen CD-Brenner sichern will, wird damit sicherlich einige Stunden verbringen.

Die Intervalle der Sicherungen muss daher jeder für sich selbst festlegen. Ich würde aber dennoch zu einer wöchentlichen Sicherung raten. Bewährt hat sich die 1-2 Methode. Hier wird in der ersten Woche ein Vollbackup gemacht. In den beiden Folgewochen sichert man nur die seit dem letzten Vollbackup hinzugekommenen Daten. Ob man dabei für die "Zwischensicherungen" auf ein differenzielles Backup oder ein inkrementelles Backup zurückgreift, hängt sicher auch von den Datenmengen ab, die gesichert werden. Einfacher im Handling beim Zurücksichern sind differenzielle Backups (siehe oben), sie benötigen aber wesentlich mehr Speicherplatz. Für die gewerbliche Umgebung ist eine tägliche Datensicherung (siehe Sicherungsplan oben) eigentlich Pflicht.

Backupmedien

Nach dem "Wie" wäre nun die Frage nach dem "Wo" zu klären.

Vorab ein Hinweis: Wer alle Backups auf ein Medium sichert, hat ein weiteres Risiko, wenn dieses Medium beschädigt ist. Gerade bei optischen Medien (CD-Brenner) würde ich nicht ständig auf das gleiche Medium sichern, sondern z.B. nach einem Vollbackup und 2 Zuwachssicherungen wechseln. Damit ist man auch gegen Mediendefekte gerüstet und baut sich gleichzeitig eine "Historie" der Daten auf. Wer ständig die einzige Sicherung durch eine neuere überschreibt, wird erst dann blass, wenn man einen Defekt an einer Datei (z.B. Word-Dokument) nach 4 Wochen feststellt und die noch funktionsfähige Datei leider schon ein paar Wochen zuvor gesichert wurde (und eventuell schon überschrieben).

Wie viele Medien zur Sicherung benutzt werden, hängt von der Wichtigkeit der Daten ab. Benutzt man die 1-2-Methode (siehe oben), kommt man in 3 Wochen mit 1 Medium aus. Mit 6 Medien könnte man daher bereits 18 Wochen Daten abbilden. Ich würde immer einen Backupsatz (Vollbackup und die folgenden Zwischenbackups) auf einem Medium speichern, damit der Medienwechsel unterbleiben kann. Im kommerziellen Umfeld würde ich die Vollbackups auch dauerhaft sichern, sofern es der Medienpreis zulässt (z.B. CDR). Gerade Buchhaltungsdaten und Rechnungen müssen 10 Jahre archiviert werden und können so gegen Verlust gesichert werden.

Keine Technik ist perfekt. Sofern möglich, sollten Sie daher die Daten nach dem Sichern immer mit den Originaldaten vergleichen lassen. Die meisten Backupprogramme bieten diese Option. Sichert man die Daten manuell oder mit einem einfachen Programm, helfen nur Programme wie z.B *DirComp*, welche Daten bitweise mit dem Original vergleichen können (sofern Sie die Daten im "Original" sichern, d.h. nicht in einem besonderen Dateiformat oder gepackt).

Festplatte

Manche Anwender sichern ihre Daten als Kopie auf einen anderen Bereich der Festplatte oder mittels eines Raid-Controllers (RAID-1 - in diesem Modus wird die aktuelle Festplatte immer auf eine 2. Festplatte gespiegelt) auf einer 2. Festplatte. Diese Art der Sicherung ersetzt kein Backup! Solange das Betriebssystem auf die Daten zugreifen kann, sind diese auch durch Viren, Systemabstürze oder versehentliches Löschen ständig gefährdet und ersetzen damit niemals ein echtes Backup auf einem Backupmedium. Allerdings sind solche Maßnahmen in Kombination mit einem Backup unter Umständen dennoch sinnvoll (z.B. *RAID1* für einen Fileserver gegen Ausfallsicherheit).

Wenn es keine andere Backupalternative gibt, sollte man zumindest auf eine andere Partition sichern. Die Sicherung auf eine andere Partition schützt zumindest vor versehentlichem Löschen oder Fehlern an der Dateizuordnungstabelle der Arbeitspartition. Sofern das Backupprogramm in eine Sicherungsdatei schreibt (und nicht die Daten im Original sichert), sind diese auch relativ sicher vor Viren und anderem Getier, da hier der Virus den gepackten Inhalt des Backups nicht lesen kann. Gegen Beschädigung oder Löschen sind diese Backups aber nicht gesichert.

Ein Wort an alle RAID-0-Nutzer. Wenngleich dieser Betriebsmodus (2 Festplatten, Daten werden abwechselnd auf beide Datenträger geschrieben) etwas mehr Performance bringt: Bei Defekt einer der beiden Festplatten sind alle Daten verloren. Die Ausfallgefahr liegt daher doppelt so hoch wie beim "normalen" Betrieb. Jeder sollte selbst beurteilen, ob der erhöhte Performance-Gewinn das Risiko wert ist.

Optische Medien

Unter optischen Medien verstehe ich CD-R(W) und DVD-R(W) in allen bekannten Formaten. CDs und DVDs zählen für den Heimbereich zu den besten Speichermedien. Für diese Sicherungsmedien sprechen die hohe Verbreitung, einfache Handhabung und günstige Medienpreise. Ob es unbedingt ein DVD-Brenner sein muss, sollte man an der Menge der zu sichernden Daten festmachen.

DVDs wie auch CDs gibt es sowohl als R- wie auch als -RW-Medium. Für die ständige Datensicherung empfehlen sich RW-Medien, da diese mehrfach überschrieben werden können. R-Medien sollten dagegen für die dauerhafte Sicherung (z.B. Buchhaltungsdaten) Verwendung finden. Allerdings lassen sich auch RW-Medien nicht beliebig oft verwenden. Viele PC-Magazine haben schon "Langzeittests" von CD-RW und DVD-RW durchgeführt und sind hier zu sehr unterschiedlichen Ergebnissen - abhängig von Hersteller und benutztem Brenner - gekommen. Im Idealfall verwendet man - gerade bei DVDs - vom Hersteller empfohlene Medien.

Um auf ein optisches Speichermedium mit jeder Backupsoftware schreiben zu können, wird im Regelfall ein *Packet-Writing-Treiber* benötigt (z.B. *InCD*). Andere Backupprogramme bringen eine eigene Brenn-Engine mit und sind damit nicht auf fremde Hilfe angewiesen.

Externe Speichergeräte ohne Wechselmedium

Dank USB2 und Firewire können Festplatten heute auch in handlichen Gehäusen extern betrieben werden. Beim Upgrade des Systems fällt da schnell eine 40-GByte-Platte ab, die sich eigentlich ideal als Backupmedium über die externen Schnittstellen eignet.

Solange das externe Speichergerät nur zur Datensicherung angeschlossen wird, ist diese Backupmethode zumindest für den Heimbereich vertretbar. Ist die Platte aber immer angeschlossen, entstehen die gleichen Gefahren wie bei der Sicherung auf die internen Festplatten (siehe Erläuterungen oben). Ein großer Nachteil liegt darin, dass man die Sicherungen nicht in einer Reihenfolge archivieren kann. Je nach Backupprogramm kann man zwar mehrere Sicherungssätze auf ein Medium schreiben; bei einem Defekt dieser Festplatte sind aber alle Sicherungen hinüber.

USB-Sticks sind zwar ein praktischer Ersatz für Disketten, zur Datensicherung aber zu teuer und zudem gefährlich. In der Eile vergisst man z.B., das Gerät zunächst abzumelden, bevor man es abzieht, und schon können die Daten auf dem Medium zerstört sein. Dies gilt natürlich auch für die oben angesprochenen USB- und FireWire-Festplatten.

Externe Speichergeräte mit Wechselmedium

ZIP-, JAZZ-, REV-Laufwerke oder Flash-Speicherkarten gehören alle zur Gruppe der externen Speichergeräte mit Wechselmedium. All diese Geräte haben gemeinsam, dass deren Medien im Vergleich zu einem optischen Speichermedium (CD oder DVD) gemessen an der Kapazität viel zu teuer sind. Für ein simples Backup sind nach meiner Meinung diese Geräte daher nicht die erste Wahl. Dafür ist das Handling im Regelfall genauso einfach wie bei der guten alten Diskette. Selbstverständlich kann man aber auch auf diese Medien seine Datensicherung machen.

Als ein Mix aus optischem Laufwerk und magnetischem Speichermedium präsentiert sich das MO-Laufwerk. Dieses findet sowohl im medizinischen als auch im forensischen Bereich starke Verbreitung. Im Heimbereich spielen diese Datenträger keine große Rolle.

Bandlaufwerke sind im Heimbereich zwischenzeitlich auch kaum noch verbreitet, sind in einer größeren IT-Umgebung aber fast ausnahmslos Sicherungsmedium Nr.1. Große Unhandlichkeit und langsame Performance haben aber viele Firmen schon dazu bewogen, eine Datensicherung auf mehrere handelsübliche Festplatten auszulagern.

Netzwerk/Internet

In Firmen werden Daten zentral auf einem Server abgelegt, der sie im Regelfall über einen RAID-1 gegen Verlust sichert. Zusätzlich werden diese Daten dann in gewissen Abständen auf ein Backupmedium gesichert.

Für das eigene LAN kann man sich viel Arbeit ersparen, wenn man auch hier die Daten zentral verwaltet, da man bei der Sicherung dann keine Daten vergisst. Wer seine Daten nur auf einen anderen Rechner im LAN kopiert, hat zwar grundsätzlich gesichert, die Daten sind aber durch Viren und Co. auch auf dem Zielrechner in Gefahr. Jedoch ist diese Art des Backups dann relativ sicher, wenn das Backupprogramm ein eigenes Dateiformat benutzt und die Dateien nicht im Original sichert (siehe Thema "Backup im Original oder eigenen Dateiformat").

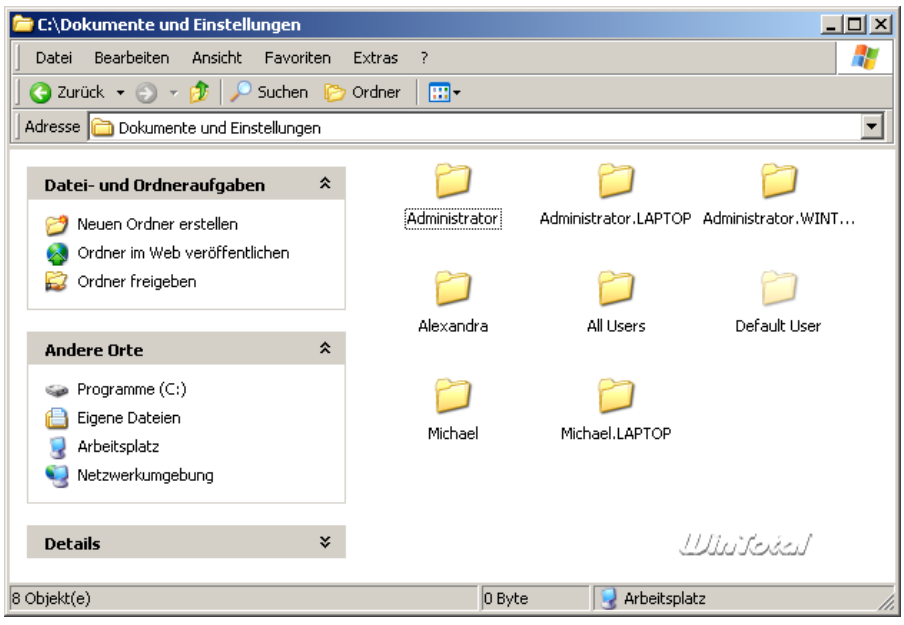
Durch höhere Uploadraten eignet sich auch ein eigener Webserver oder einfacher Webspace zur Sicherung der wichtigsten Daten. Mit Programmen wie *VirtualDrive* oder *WebDrive* können FTP-Speichermöglichkeiten auch als lokale Laufwerke eingebunden und damit für jedes Backupprogramm zugänglich gemacht werden. Allerdings würde ich persönliche Daten nicht unverschlüsselt außerhalb des eigenen Zugriffsbereichs aufbewahren.

Sicherung von Daten

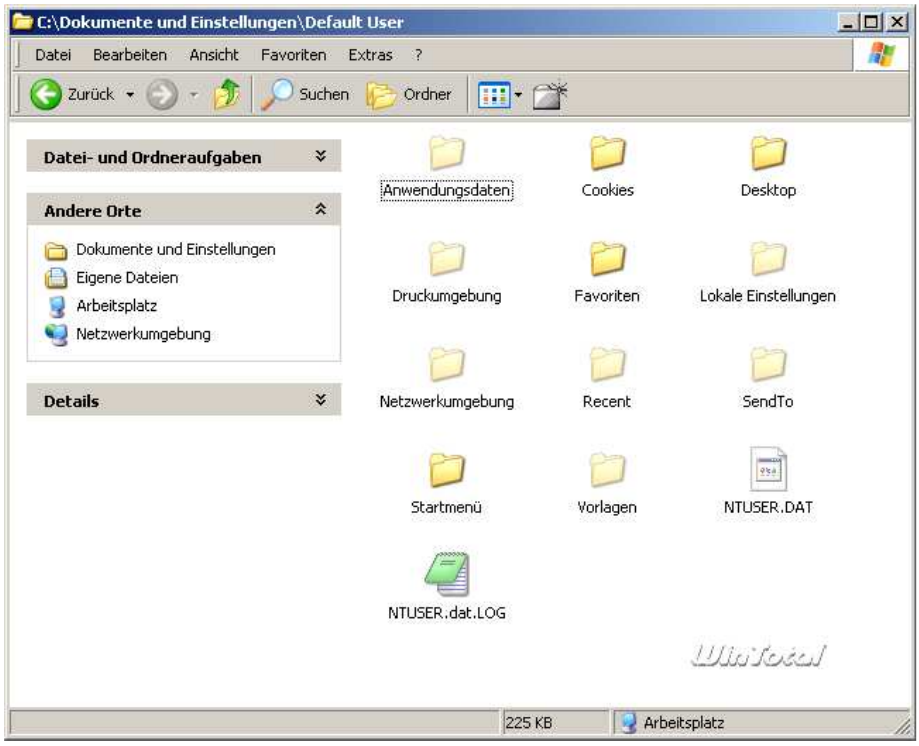
Wo sind die Daten

Damit man seine Daten auch alle sichert, müssen diese erstmal gefunden werden. Dummerweise liegen diese keineswegs alle zentral an einem Platz.

Seit Windows2000 werden alle Benutzerdaten unter "Dokumente und Einstellungen" auf dem Systemlaufwerk gespeichert. Hier finden sich Ordner der einzelnen Benutzer.



In den Benutzerordnern finden sich weitere Unterordner:

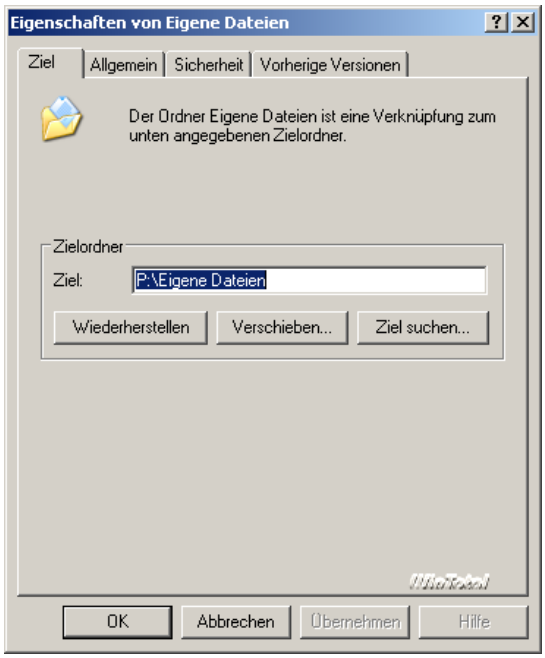


Alle Ordner werden nur sichtbar, wenn unter den Optionen versteckte Systemordner auch angezeigt werden.

- ✓ Die Ordner *Favoriten* und *Cookies* sind selbsterklärend.
- ✓ Der Ordner *Vorlagen* ist nur vorhanden, wenn auch Microsoft Office installiert ist.
- ✓ Der Ordner *Desktop* beinhaltet alle Dateien und Verknüpfungen, die auf dem Desktop zu sehen sind.
- ✓ *SendTo* bildet "Senden an" ab.
- ✓ *Druckerumgebung* und *Netzwerkumgebung* speichert im Netzwerk gefundene Ziele.
- ✓ *Startmenü* beinhaltet das Startmenü des Benutzers.
- ✓ Im Ordner *Lokale Einstellungen* finden sich die temporären Internetdateien (Cache), Verlauf, Temp-Verzeichnis und Anwendungsdateien einiger Applikationen. In diesem Ordner speichert z.B. auch Outlook Express die Dateien des jeweiligen Nutzers ab.
- ✓ Im Ordner *Anwendungsdaten* werden ebenfalls benutzerspezifische Einstellungen diverser Applikationen, u.a. vom Internet-Explorer, abgelegt. In diesem Ordner findet sich auch das Adressbuch von Windows.

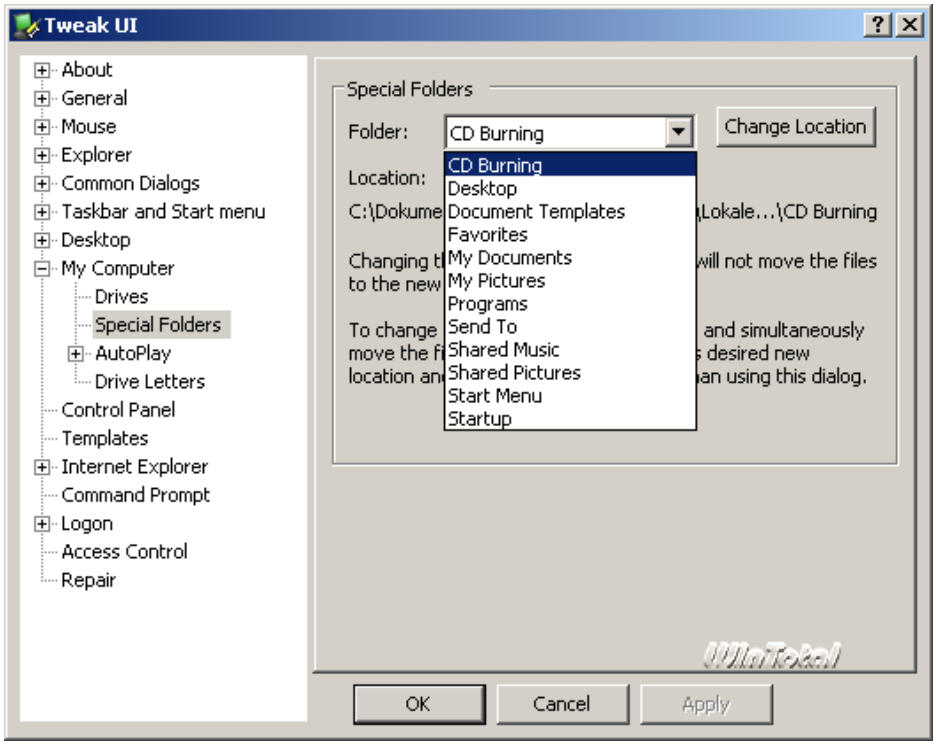
Der wichtigste aller Ordner ist "Eigene Dateien", welcher auch die Unterordner "Eigene Musik", "Eigene Filme", "Eigene Bilder" und anderen Kram enthält.

Je nach verwendeter Windows-Version findet sich der Ordner an verschiedenen Stellen, jedoch immer auf dem Windows-Laufwerk. Sie können über das Kontextmenü -> Eigenschaften des Ordners "Eigene Dateien" auf dem Desktop selbst herausfinden, wo sich der Ordner befindet.



Der Ordner lässt sich mit dem Inhalt auch über den entsprechenden Button verschieben. In der Praxis hat sich bewährt, dass man System und Dateien trennt und die Daten auf einer 2. Partition speichert. Auf diese Möglichkeit und die Umsetzung geht der 2. Teil dieses Artikels ein.

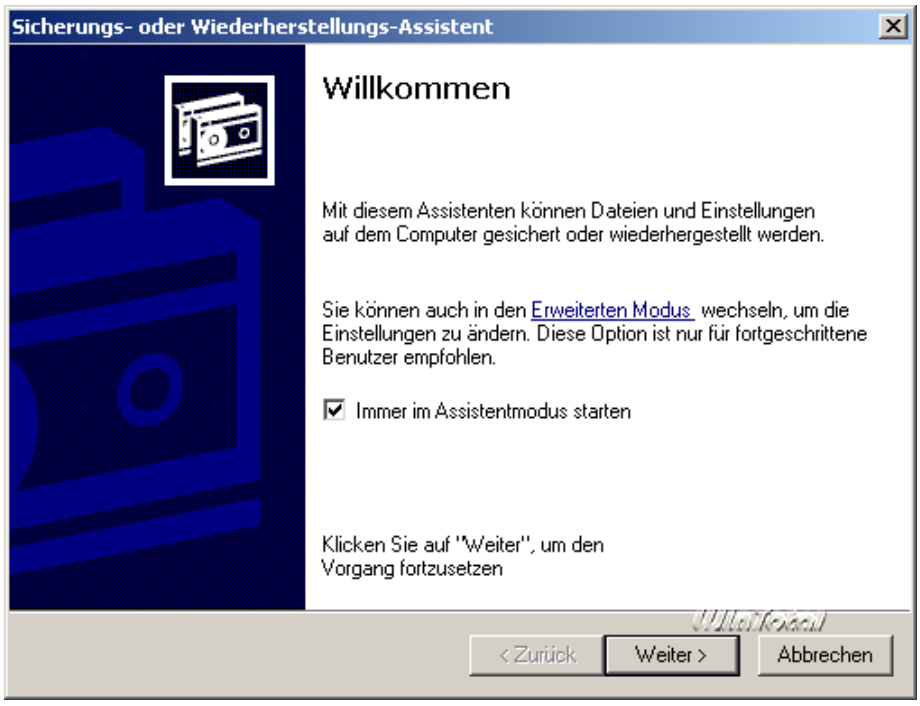
Auch *TweakUI-XP* (Windows XP und 2003 Server) bzw. *TweakUI-2000* (Windows 9x und Windows 2000) helfen beim Finden von Speicherordern, wenn diese z.B. durch eine Vorinstallation an andere Stelle gelegt wurden.



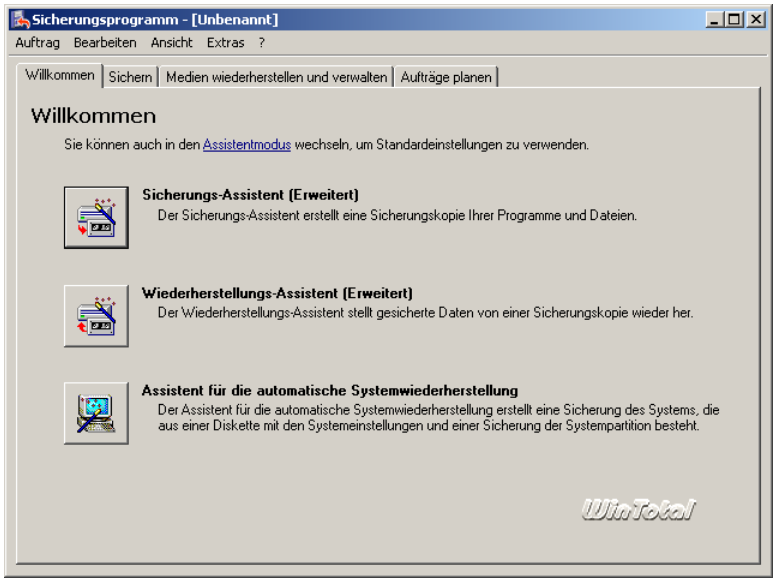
Wer sicher gehen möchte, sichert den eigenen Ordner unterhalb "Dokumente und Einstellungen" komplett. Allerdings ist hier auch viel Dateimüll (*Temp-Ordner*, *Internetcache*, *Verlauf, Cookies* etc.). Wichtig sind mit Sicherheit *Eigene Dateien*, *Favoriten*, *Desktop* und der Ordner von *Outlook Express* unterhalb von Anwendungsdateien sowie das Adressbuch. Wer andere Programme benutzt, muss prüfen, wo diese ihre Dateien ablegen.

Sicherung mit Windows Backup

Windows bringt seit Windows98 ein recht brauchbares Backupprogramm mit, welches zuvor auch von *Veritas* mit erweitertem Funktionsumfang vertrieben wurde. Das größte Manko von *Windows-Backup* ist die fehlende Softwarekomprimierung. Unter Windows XP findet sich das Windows-Backup unter dem Namen "Sicherung" unter Zubehör -> Systemprogramme.

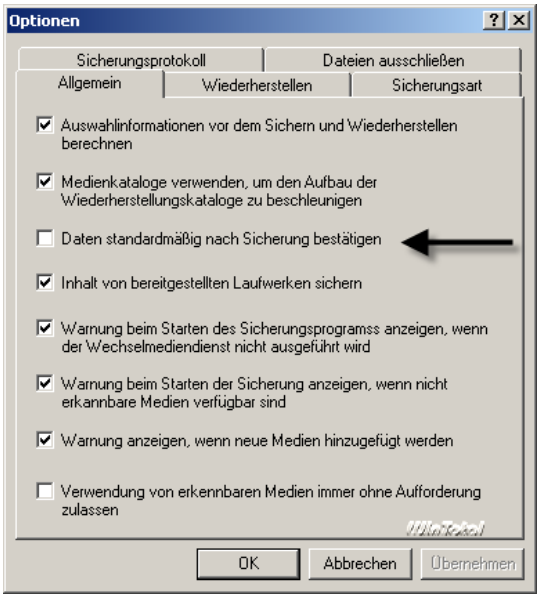


Das Programm startet im *Assistentenmodus*, kann aber auch in den "*Erweiterten Modus*" wechseln und zeigt so alle Funktionen.

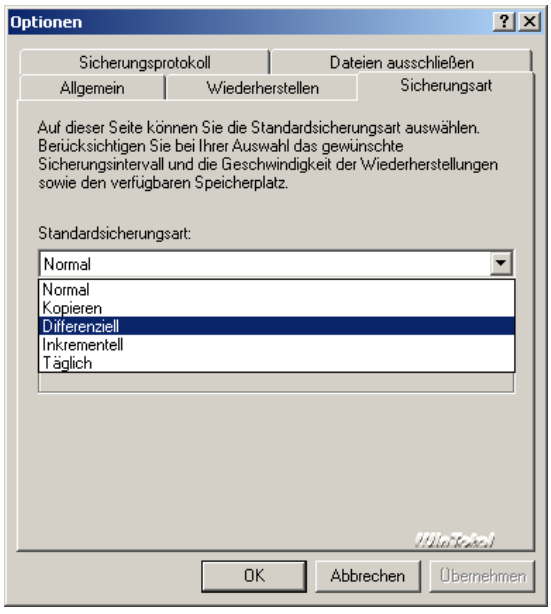


Die Bedienung ist zusammen mit der Hilfsfunktion eigentlich selbsterklärend. Dennoch möchte ich einige Anmerkungen geben.

- ✓ Damit das Programm auch auf optische Medien wie CDR oder CDRW schreiben kann, muss ein Packet-Writing-Treiber installiert und das Medium schreibbereit sein. Nur dann kann das Programm auf den Datenträger schreiben.
- ✓ Da das Programm keine Daten komprimiert, sollte man größere Mengen von Word-Dokumenten o.Ä. unter Umständen bereits gezippt auf der Festplatte speichern. Die NTFS-Komprimierung bringt hier nichts, wenn die Daten auf die CD wandern. Als Sicherungsart muss hier übrigens Datei gewählt werden.
- ✓ Das Sicherungsprogramm kann auch die Dateien nach dem Sichern dahingehend prüfen, ob sie mit den Originaldateien identisch sind (Fehler ausschließen). Die entsprechende Option findet sich unter Extras -> Optionen auf der Registerkarte Allgemein als 3. Auswahlpunkt.



- ✓ Die Sicherungsart (siehe Anfang des Artikels) lässt sich unter Extras -> Optionen -> Sicherungsart festlegen.



Sicherung per Batch-Datei

Wer es gerne spartanisch mag, kann auch altbekannte Funktionen nutzen: *XCOPY*.

Mit der einfachen Befehlszeile

xcopy %Source% %target% /s /c /i /f /h /k /o /x /y

kann man bereits ein Vollbackup machen.

Für *%Source%* und *%Target%* muss man zuvor in einer Batch-Datei per SET-Befehlen die Pfade vorgeben, z.B. Set Source="C:\Dokumente und Einstellungen\Michael"SetTarget="X:\Backup ".

Die Parameter hinter *XCOPY* werden auch durch *xcopy /?* In der Eingabeaufforderung erläutert.

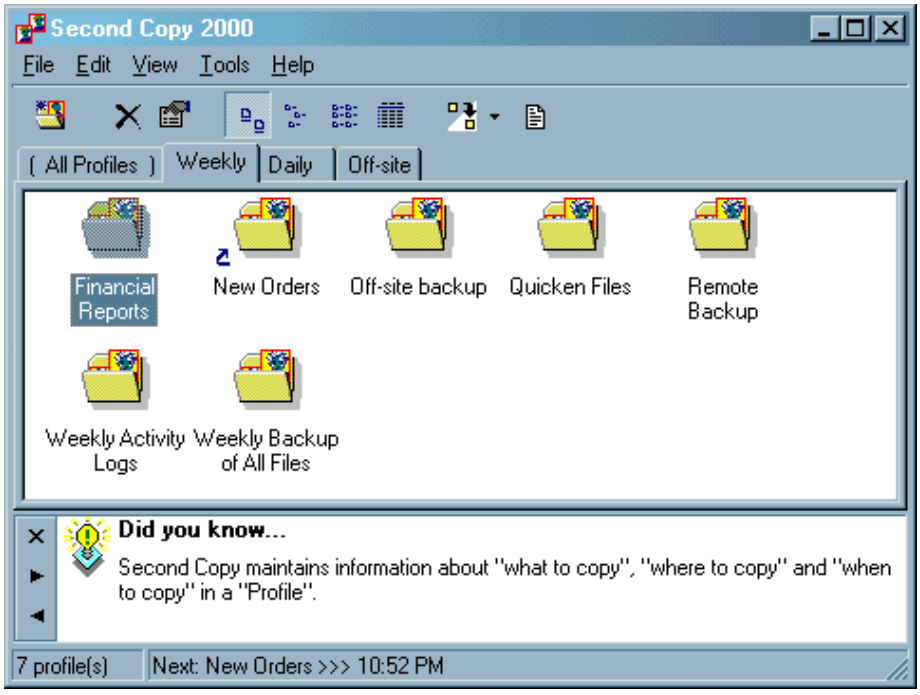
Die Sicherung per Batch in dieser Form ist nicht sonderlich bequem.

Achtung: Das Script sichert nur beim ersten Aufruf alle Dateien und danach nur noch inkrementell, d.h. die Veränderungen von Sicherung zu Sicherung. Verantwortlich hierfür ist der Parameter /m in der XCOPY-Befehlszeile, da dieser nur Dateien mit dem Attribut "a" sichert. Wer dies nicht möchte und stattdessen immer ein Vollbackup erzeugen möchte, muss den Parameter löschen.

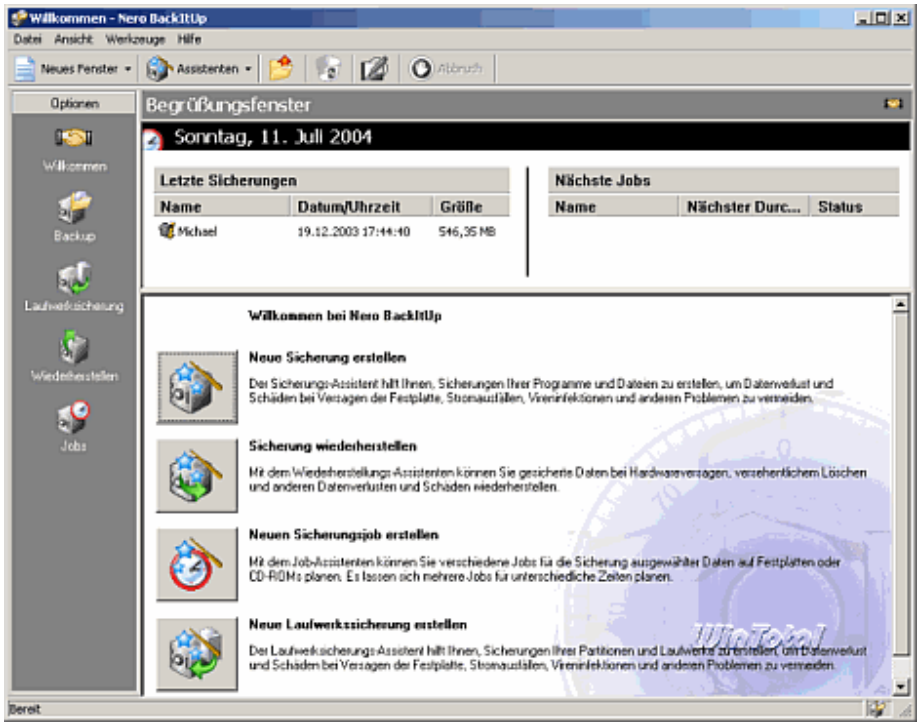
Weitere Programme

Die Zahl der Backupprogramme auf dem Markt ist nicht mehr überschaubar. *AdBackup*, *Backup4all*, *TaskZip* und *EZBack-it-up* haben sich als Freeware in der Praxis besonders bewährt, bieten aber alle eine andere Handhabung und Sicherungsansätze.

Aus dem Sharewarelager halte ich *Second Copy* für besonders interessant. Wie *TaskZip* arbeitet das Programm mit Sicherungsprofilen, welche sich sehr individuell anpassen lassen und die Dateien (auf Wunsch gepackt) im Originalformat sichern.



Besitzer von *Nero6* bekommen mit *Nero Backit Up* ein sehr gutes Backupprogramm, welches sich zur Sicherung auf DVD und CD eignet. Es bietet neben einem *Scheduler* auch Komprimierung und ist daher eine gute Alternative zum *Windows-Backup*.



Sicherung des Systems

Viren, Würmer, störrische Treiber und fehlerhafte Programme bringen selbst Windows XP aus dem Tritt. Läuft irgendwann etwas schief, kann man sich lange mit der Fehlersuche beschäftigen oder alles neu installieren. Die Einrichtung des Betriebssystems mit allen Treibern, Applikationen und Einstellungen dauert aber selbst im schnellsten Fall bereits einige Stunden. Zudem müsste man sich für jede Neuinstallation vorher notieren, was man eigentlich alles eingerichtet und installiert hat. Ideal wäre daher, wenn man auch vom System eine Sicherung erstellt.

Mit den vorausgegangenen Backuplösungen kann man das laufende Betriebssystem im Regelfall aber nicht sichern, da Windows geöffnete Dateien exklusiv sperrt und nur ein kleiner Kreis von Image-Programmen ein laufendes System überhaupt sichern kann. Zudem macht es auch wenig Sinn, das Betriebssystem im gleichen Rhythmus wie die eigenen Dateien zu sichern, da sich am System selbst im Regelfall nach der vollständigen Installation und Einrichtung nur wenig ändert.

Speziell für die Sicherung des Systems gibt es so genannte **Image-Programme**.

Beim Sichern wird ein genaues Abbild der gewählten Partition auf eine andere kopiert oder in eine so genannte Image-Datei geschrieben. Um die Größe solcher Image-Dateien klein zu halten, werden im Normalfall nur Sektoren kopiert, die auch belegt sind. Eine 10 GByte-Partition, welche nur mit 2 GByte belegt ist, benötigt so maximal 2 GByte als Image-Datei. Zusätzlich bieten Image-Programme beim Schreiben einer Image-Datei noch die Option der Komprimierung in mehreren Stufen. Dadurch wird die Größe einer Image-Datei je nach Dateitypen auf der Partition nochmals um bis zu 40 Prozent reduziert. Die Image-Datei kann man natürlich auch auf einen Brenner oder andere Wechselmedien sichern. Dazu splitten die Programme die Image-Datei in mehrere Stücke, welche einzeln je auf ein Medium passen.

Sollte das Betriebssystem nach einer gescheiterten De- oder Installation oder aus anderen Gründen wie Virenbefall etc. beschädigt sein, kann das zuvor gesicherte Abbild der Partition einfach wieder zurück geschrieben werden.

Problem: Trennung Daten und System

Sichert man sein System vom Laufwerk C und spielt dieses wieder zurück, sind damit auch alle Dateien verloren, welche seit dem Image hinzugefügt wurden. Der beste (und einzige praktikable) Weg ist daher die Trennung von Daten und System. Dies erfordert zum einen mindestens eine 2. Partition (für die Daten) und zum anderen Kenntnis, wo Windows welche Dateien speichert, da das Betriebssystem und die Applikationen gerne ungefragt ihre Daten irgendwo im Ordnerdschungel von Windows ablegen.

Eigene Datenpartition erstellen

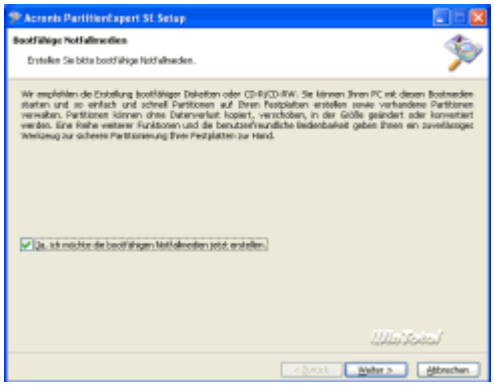
Wenn noch keine eigene Datenpartition existiert oder diese zu klein ist, kann in beiden Fällen mit kommerziellen Programmen wie *Partition Magic* oder *Acronis Disk Director Suite 9.0* Abhilfe geschaffen werden. Es gibt auch Freeware wie *Partition Resizer*. Diese läuft allerdings nur unter *DOS*, ist nicht sonderlich komfortabel zu bedienen und auch nicht so leistungsfähig.

Eine weitere Alternative ist die Vollversion von *Acronis Partition Expert 2003 SE*. Hierbei handelt es sich um den Vorgänger der *Acronis Disk Director Suite*, der sich als *SE-Version* aber nur im Assistentenmodus bedienen lässt.

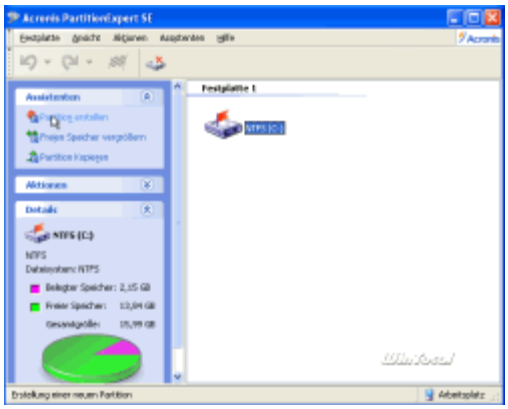
Acronis Partition Expert 2003 SE ermöglicht es, Partitionen in der Größe zu ändern, zu kopieren und ohne Datenverlust zu verschieben, den belegten Speicherplatz auf der Festplatte zu optimieren und viele andere Partitionierungsaufgaben zu übernehmen. *Acronis'* exklusive Dateisystemunterstützung beinhaltet *Windows FAT16, FAT32, NTFS, Linux Ext2, Ext3, ReiserFS*, und Linux *Swap*.

Weitere Partition mit Acronis *Partition Expert 2003 SE* erstellen

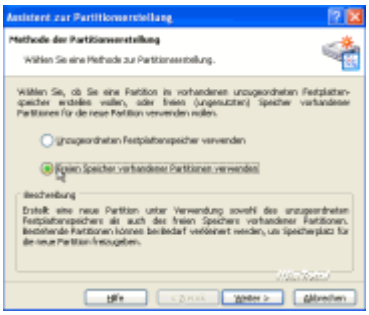
Beispielhaft an einem Test-Windows wird gezeigt, wie man mit diesem Programm eine 2. Partition erstellt. Während der Installation kann man noch ein bootfähiges Medium erstellen, was sich für Wartungsarbeiten sehr empfiehlt.



Nach dem ersten Start präsentiert sich das Programm mit 3 Funktionen, da sich die SE-Version nur im Assistentenmodus starten lässt. Für unsere Aufgaben (Partition erstellen oder bestehende in der Größe ändern) reicht dies aber aus.

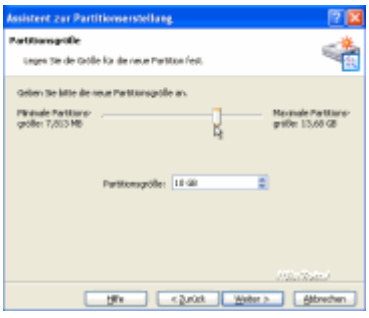


Der Assistent für das Erstellen einer Partition möchte im folgenden Dialog wissen, ob er den Platz aus der bestehenden Partition oder aus nicht zugeordnetem Speicher nehmen soll. Im Regelfall dürfte kein nicht zugeordneter Speicher auf der Festplatte vorhanden sein, so dass Punkt 2 auszuwählen ist.



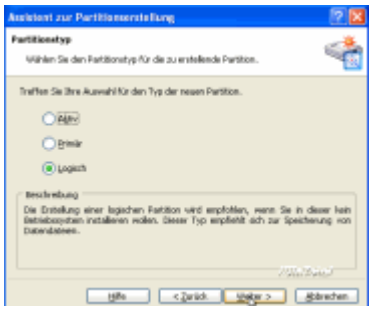
Nun wählt man die erste Partition aus und klickt auf "Weiter". Die Software versucht nun die Partition zu sperren. Sollte dies nicht gelingen, startet man das Programm im exklusiven Modus. Alternativ kann man alles auch mit dem Bootmedium durchführen.

Jetzt legt man fest, wie groß die neue Partition nach der Änderung sein soll. Je mehr Platz Sie hier angeben, desto kleiner wird später das Systemlaufwerk (hier C). Lassen Sie bitte aber mindestens 2 GByte auf dem Systemlaufwerk noch frei, da das Betriebssystem neben der Auslagerungsdatei auch temporäre Dateien anlegt und freien Speicher so kurzfristig immer belegt.



Der nächste Dialog ist sehr wichtig. Bitte lesen Sie den folgenden Absatz daher unbedingt durch!

Das Programm möchte nun wissen, welcher Partitionstyp für die neue Partition vergeben werden soll. Bitte wählen Sie "logisch". Das Programm erstellt dann selbstständig eine erweiterte Partition und darin das logische Laufwerk. "Primär" würde dazu führen, dass es 2 primäre Partitionen auf einem Laufwerk gibt. Nicht alle Betriebssysteme und Programme können damit fehlerfrei umgehen.

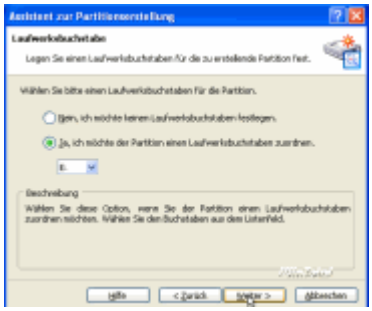


Als Dateisystem sollten Sie NTFS verwenden. FAT32 macht nur dann Sinn, wenn Sie auf die Daten auch mit älteren Betriebssystemen wie Windows 9x/ME oder DOS zugreifen müssen.

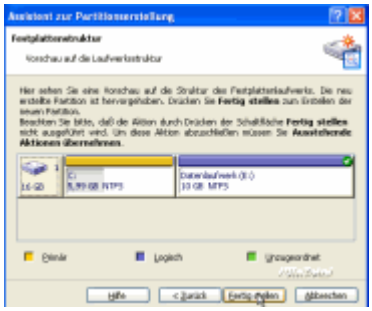
Zuletzt legt man noch den Laufwerksbuchstaben für die neue Partition fest. Bei NTFS kann jeder beliebige Buchstabe zugeordnet werden. Nutzt man FAT32, vergibt das Betriebssystem den Buchstaben nach der Reihenfolge der primären und erweiterten Partitionen selbstständig.

Achtung: Man sollte nach Möglichkeit keinen Buchstaben, der bereits für ein weiteres Laufwerk verwendet wurde, wählen. Sonst würde bereits installierte Software, die z.B. von CD Daten nachladen muss, nicht mehr richtig funktionieren, da an der Stelle nun eine Festplatte statt z.B. dem DVD-ROM zu finden ist.

In unserem Beispiel wählen wir E für die neue Partition, da D bereits von einem CD-ROM benutzt wird.

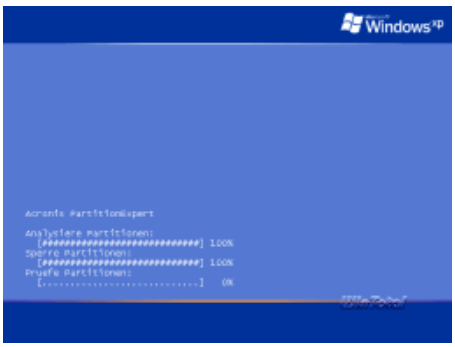


Zuletzt legt man die Datenträgerbezeichnung fest, worauf *Partition Expert 2003 SE* eine Zusammenfassung bringt:



Wie man sieht, wird nach dem Klick auf "*Fertig stellen*" die Festplatte in 2 Partitionen geteilt. Das C-Laufwerk wird erst um 10 GByte verkleinert und in dem frei gewordenen Speicherplatz ein neues Laufwerk (E) erstellt. Durchgeführt wird die Aktion aber erst, wenn Sie im Hauptprogramm auf die "Rennfahne" klicken. Das Programm muss dann den Rechner neu starten, um die Änderungen auszuführen.

Beim nächsten Systemstart zeigt *Partition Expert* einige Textmeldungen und führt die Änderungen an der Festplatte durch.



Gibt es beim Ausführen des Programms an einer Stelle Probleme (z.B. kann die Partition nicht gesperrt werden), führen Sie alle Aktionen mit dem Bootmedium von Partition Expert aus, welches Sie auch nachträglich über den Eintrag im Startmenü von Windows erstellen können.

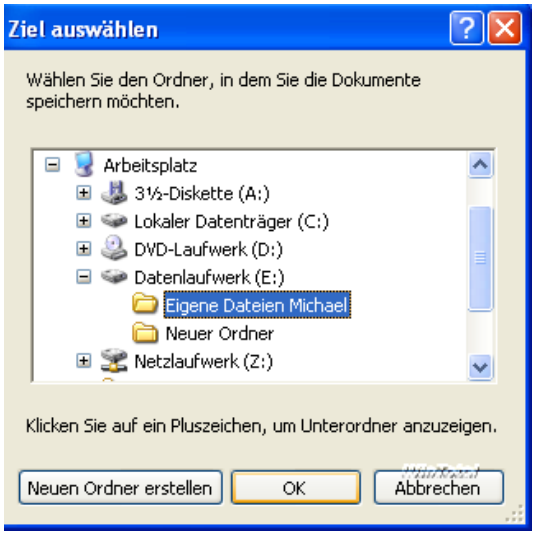
Nach dem Warmstart muss Windows das System aber nochmals starten, da die neue Partition nun gefunden wurde. Ab dann ist die neue Partition einsatzbereit.

Ändern von Systempfaden auf die neue Partition

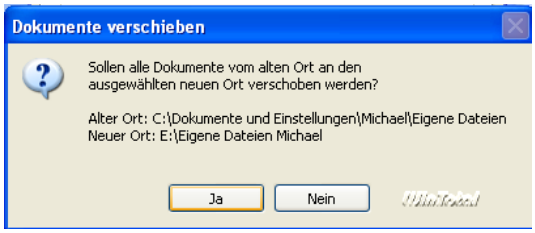
Nachdem die neue Partition jetzt erstellt (oder vergrößert) wurde, muss das Betriebssystem gezwungen werden, alle Daten auch auf diesem Laufwerk abzulegen. Leider ist dies nicht so einfach, das es keine gemeinsame Schaltzentrale für alle Systempfade gibt.

Der wichtigste aller Ordner ist zweifelsohne "Eigene Dateien" eines jeden Benutzers. Dieser kann von Windows selbst verschoben werden. Dazu klickt man mit der rechten Maustaste über dem Ordner "Eigene Dateien" auf dem Desktop oder im Startmenü von Windows XP, um das Kontextmenü des Ordners zu öffnen, wählt hier "Eigenschaften" und dann "Verschieben".

Es öffnet sich ein weiterer Dialog, der den Zielpfad abfragt. Hier wählt man das neu erstellte Laufwerk. **Man sollte unbedingt einen Unterordner (hier "*Eigene Dateien Michael*"), da sonst alle Dateien ins Hauptverzeichnis der Festplatte kopiert werden, was zu Problemen (insbesondere bei mehreren Nutzern) führen kann**. Zudem erleichtern mehrere Ordner für verschiedene Benutzer später die Datensicherung und Zuordnung.



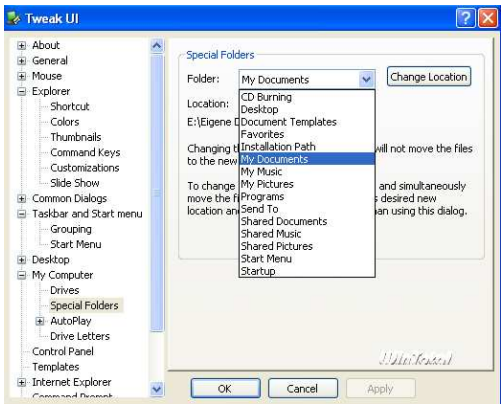
Ein Ja/Nein-Dialog möchte nun wissen, ob die Dateien des bisherigen Ordners "*Eigene Dateien*" in den Zielordner verschoben werden sollen



Dies war auch unser Ziel und wir bestätigen den Dialog mit "Ja".

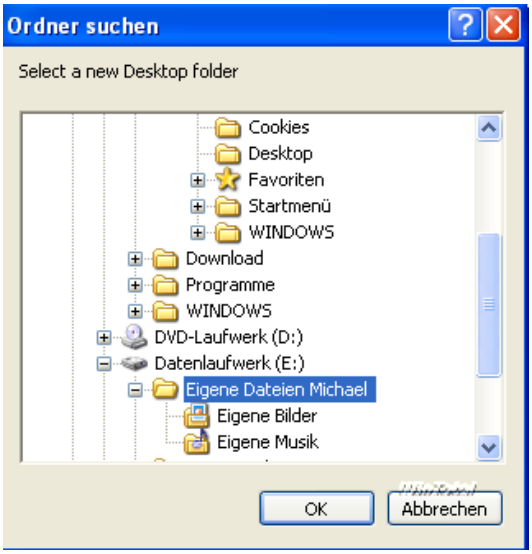
Windows kopiert nun alle Ordner und Dateien vom Ordner "*Eigene Dateien*" des Benutzers an das neue Ziel. Gleichzeitig ändert das System auch die Pfade für "*Eigene Musik*" und "*Eigene Bilder*".

Damit sind wir allerdings noch nicht am Ziel. Im Folgenden möchten wir noch weitere Ordner an das neue Ziel verschieben. Zu diesem Zweck installieren Sie am besten *TweakUI für Windows XP* (bzw. die ältere Ausgabe für andere Systeme) und navigieren dann unter "*My Computer*" -> "*Special Folders*".



Über "*Change Location*" kann man nun bequem jeden der *Special Folder* an einen neuen Platz legen. Letztlich ändert *TweakUI* aber nur *Registry-Einträge*, die sich für jeden Benutzer auch in der *Registry* unter *HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Explorer \Shell Folders* finden.

***TweakUI* verschiebt keine Ordner**. Zudem bietet der Change-Location-Dialog keine Option, einen neuen Ordner am Ziel zu erstellen.



Man muss daher vorab jeweils den Ordner am Ziel erstellen. Möchten man z.B. den Ordner Favoriten (welcher die Favoriten des Internet-Explorers beinhaltet) auch als Unterordner unter "*Eigene Dateien*", dann kopieren Sie am besten den ganzen Ordner Favoriten zunächst in den Ordner "*Eigene Dateien*" auf dem Datenlaufwerk. Danach ändert man mit *TweakUI* den Pfad auf diesen neuen Ordner. Nach einem Neustart (bzw. einer Abmeldung) nutzt Windows dann den *Favoriten-Ordner* an der neuen Position. Jetzt kann man den alten *Favoriten-Ordner* löschen.

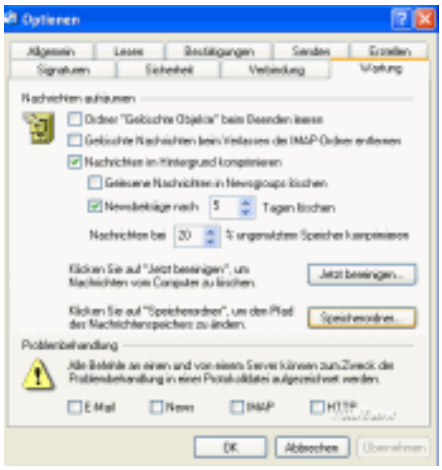
Welche weiteren Ordner auf das Datenlaufwerk ?

Neben dem Ordner "*Eigene Dateien*" lohnen sich folgende Ordner - ebenfalls als Unterordner von "Eigene Dateien" - auf dem Datenlaufwerk:

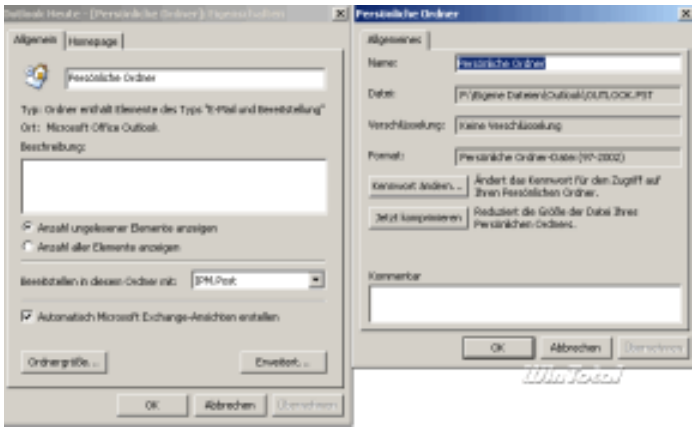
- ✓ **Favoriten:** Dieser Ordner beinhaltet alle Favoriten des Internet Explorers. Er findet sich normalerweise unter "Dokumente und Einstellungen / Benutzername"
- ✓ **Desktop**: Alle Verknüpfungen zu Programmen oder Webseiten, die auf dem Desktop liegen, speichert Windows in einem Ordner "Desktop" unter "Dokumente und Einstellungen / Benutzername". Viele nutzen den Desktop aber auch "mac like", d.h. als Datenablage von neuen Dokumenten etc. Ich würde daher raten, auch den Desktop-Ordner auf das neue Datenlaufwerk als Unterordner von "Eigene Dateien" zu legen.
- ✓ **Cookies und Verlauf:** Wer möchte, kann auch Cookies und Verlauf auf das neue Laufwerk legen. In diesem Fall erstellen Sie wieder namensgleiche Ordner im neuen Ordner "Eigene Dateien" durch Kopie der Originalordner und ändern dann mit TweakUI die Pfadangaben. Der Verlauf findet sich unter "C:\Dokumente und Einstellungen\ Benutzername\ Lokale Einstellungen", die Cookies unter "C:\Dokumente und Einstellungen\ Benutzername\".

Weitere Ordner, deren Pfadangaben über die Registry oder das jeweilige Programm selbst geändert werden müssen:

- ✓ **Adressbuch:** Das Adressbuch von Windows/Outlook Express liegt normalerweise unter "*C:\Dokumente und Einstellungen\ Benutzername\ Anwendungsdaten\ Microsoft\ Address Book*". Kopieren Sie die darin befindliche *WAB-Datei* in einen neuen Ordner unterhalb von "*Eigene Dateien*" (z.B. Adressbuch). Anschließend muss man diesen neuen Pfad in der *Registry* unter *HKEY_CURRENT_USER\ Software\ Microsoft \WAB\ WAB4 \Wab File Name* vollständig angeben.
- ✓ **Outlook-Express:** Outlook Express kann die Mails selbstständig an einen neuen Ort kopieren. Man erstellt zuerst unterhalb von "*Eigene Dateien*" einen neuen Ordner (z.B. *Mails*). Dann startet man Outlook Express. Unter Extras -> Optionen -> Wartung kann man mit dem Button "*Speicherordner*" den neuen Zielpfad angeben. Outlook Express kopiert nun alle Daten in diesen Ordner. Nach einem Neustart sollte der neue Ordner benutzt werden.



- ✓ Outlook: Outlook legt die *PST-Datei* je nach Version an verschiedenen Stellen ab. Man sucht die *PST-Datei*. Den Pfad erfährt man beispielsweise, wenn man Outlook starten, die Eigenschaften des "*Persönlichen Ordners*" aufrufen (Kontextmenü) und dann auf "*Erweitert*" klickt.



Beende das Programm und verschiebe die *PST-Datei* an den neuen Ort, z.B. in einen Ordner "*Outlook*" als Unterordner von "*Eigene Dateien*".

Starte nun wieder Outlook. Das Programm moniert nun das Fehlen der *PST-Datei* und möchte den Pfad wissen. Hier gibt man nun dem Programm den neuen Pfad zur *PST-Datei* an.

- ✓ **Internet-Cache und Temp-Verzeichnis**: Sowohl der Internet-Cache des Internet Explorers als auch das Temp-Verzeichnis liegen normalerweise auf dem Systemlaufwerk. Man kann beide auch auf das Datenlaufwerk legen. Für das Temp-Verzeichnis muss man dann unter "*System*" in der Systemsteuerung bei "*Erweitert*" in den Umgebungsvariablen den Pfad selbst ändern.

- ✓ **Ordner „Gemeinsame Dokumente“:** Der Ordner Gemeinsame Dokumente, welcher vor allem unter Windows XP Home bei mehreren Benutzern Verwendung findet, kann auch auf das neue Laufwerk gelegt werden.

Will man weitere Ordner auf das Datenlaufwerk legen, sucht man in den Optionen der Programme nach einer Möglichkeit. Viele Programme bieten diese Funktion. Sonst hilft auch ein Blick in die *Registry*. Für Windows finden sich viele Pfadangaben *unter HKEY_CURRENT_USER\ Software\ Microsoft\ Windows \CurrentVersion\ Explorer\ Shell Folders.*

Ordner "Dokumente und Einstellungen"

Windows 2000 und XP speichern alle Profile (und somit Benutzerdaten und Einstellungen) auf dem Laufwerk *Windir:\Dokumente* und *Einstellungen*. Man kann diesen Ordner bereits bei der Installation angeben, wenn man dazu eine "*Unattend"-Installation* startet.

Ist Windows bereits installiert, empfehle ich die folgende Methode nur im Ausnahmefall. Generell reicht es, wenn - wie oben beschrieben - die wichtigsten Ordner auf dem Systemlaufwerk liegen.

Verschieben man allerdings den ganzen Ordner "Dokumente und Einstellungen", brauchen man die Ordner "*Eigene Dateien*" und Co. nicht noch mal zu verschieben.

Den ganzen Ordner „*Dokumente und Einstellungen*“ verschiebt man wie folgt:

- Im Arbeitsplatz/Explorer müssen unter Ordneroptionen/Ansicht ALLE (auch versteckte) Dateien sichtbar gemacht werden.
- Man erstellt auf dem Wunschlaufwerk einen neuen Ordner und merkt sich den Pfad. Da in der Registry fast immer "Dokumente und Einstellungen" verwendet wird, ist es am einfachsten, wenn man einen gleichen Ordner auf einem anderen Laufwerk erstellt. So braucht man später nur einen Wert in der Registry zu ändern.
- Beim Erstellen des neuen Ordners ist zu beachten, dass das System unbedingt Zugriff auf diesen haben muss (Dokumente und Einstellungen), bevor man weitere Operationen vornimmt. Die Vererbung sollte aktiviert bleiben, sonst kann das Benutzerprofil beim nächsten Neustart nicht geladen werden.
- Jetzt wechselt man in den Original-Ordner „Dokumente und Einstellungen“ (als Administrator) und markiert dort alle Profilordner der **Benutzer**. Diese kopiert man in den neu erstellten Ordner auf dem Wunschlaufwerk.
- Jetzt wechselt man in die Systemsteuerung auf System-> Benutzerprofile. Hier kopiert man das Profil des aktuell angemeldeten Benutzers ebenfalls in den neuen Ordner (nicht vergessen, zuerst einen Ordner für den aktuellen Benutzer zu erstellen).
- Zuletzt startet man REGEDIT.
- Der eigentliche Pfad für *%Userprofile%* wird in der *Registry* im Schlüssel *HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows NT\ CurrentVersion\ ProfileList* gespeichert. Ändert man hier einfach den Laufwerksbuchstaben bei dem Wert *ProfilesDirectory*. Damit sind alle relativen Pfade, die normalerweise *%userprofile%\ Dokumente und Einstellungen* lauten, auf dem neuen Laufwerk.
- Sucht man zudem in der *Registry* nach "*Dokumente und Einstellungen*" und ändert alle Werte, die *C:* oder *%systemdrive%* beinhalten, auf das neue Laufwerk (nicht aber für die Benutzer *LocalService* und *NetworkService*).
- Nach einem Neustart kann man dann die alten Ordner löschen.

Weitreichender als mit *TweakUI* kann man auch in der *Registry* einzelne Ordner manuell auf neue Ziele legen.
Unter *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserShellFolders* gelten folgende Werte:

Name: AppData
Type: REG_EXPAND_SZ
Data: %USERPROFILE%\Application Data

Name: Desktop
Type: REG_EXPAND_SZ
Data: %USERPROFILE%\Desktop

Name: Personal
Type: REG_EXPAND_SZ
Data: %USERPROFILE%\My Documents

Name: My Pictures
Type: REG_EXPAND_SZ
Data: %USERPROFILE%\My Documents\My Pictures

Name: Start Menu
Type: REG_EXPAND_SZ
Data: %USERPROFILE%\Start Menu

Default-Einstellungen für neue Benutzer

Möchte man die Ordner für neue Benutzer automatisch ändern, müssen die Werte auch unter HKEY_USERS\ .DEFAULT\ Software \Microsoft\ Windows\ CurrentVersion\ Explorer\ User Shell Folders und *HKEY_USERS\ .DEFAULT\ Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\ Shell Folders* auf das neue Laufwerk geändert werden.

Sicherung in Image-Datei

Nachdem wir nun Daten und System getrennt haben, kann das Betriebssystem mit einem Image-Programm gesichert werden. Bekannte Vertreter sind *DriveImage* von ehemals PowerQuest, *Ghost* von Symantec oder *TrueImage* von Acronis. Aus dem Freewarelager bietet sich *PartitionSaving* an, welches aber nur unter *DOS* arbeitet. Eine günstige Alternative ist die Vollversion von Acronis *TrueImageSE*.

Die auf der CD befindliche Vollversion entspricht in etwa der Version 6 von *TrueImage*, kann allerdings nicht auf DVD-, USB-, Firewire- oder Netzwerklaufwerke schreiben. Zumindest kann man sein Image aber auf die 2. Partition sichern und von dort auf CD/DVD brennen.

Das Sichern in eine Image-Datei ist selbsterklärend, so dass wir nicht näher darauf eingehen.

Für zwischendurch: Systemwiederherstellung

Mit Hilfe der Systemwiederherstellung kann man einen PC zu einem bestimmten Zeitpunkt wiederherstellen. Das bedeutet, wenn der PC vor der Installation eines bestimmten Programms noch lief, kann man den PC in den Zustand bringen, in dem er vor der Installation dieses Programms war.

Die Systemwiederherstellung merkt sich den aktuellen Zustand der zu überwachenden Festplatten und speichert ab dem Zeitpunkt des Systemwiederherstellungspunktes alle folgenden Veränderungen (gelöschte und überschriebene Dateien sowie veränderte Dateien). Die Systemwiederherstellung kann man sowohl im *abgesicherten* als auch im *normalen Modus* benutzen. Im normalen Betriebsmodus erreicht man sie unter *Start->Programme->Zubehör->Systemprogramme->Systemwiederherstellung*.

Hier kann man den Systemwiederherstellungspunkte erstellen oder zu einem bereits erstellten wieder wechseln. Die Funktion von Windows merkt sich nur die Veränderungen von Systempunkt zu Systempunkt. Man kann auch chronologisch das System zurücksetzen. Will man also z.B. zu einem Systempunkt am 01.10.2003 wechseln, werden alle Änderungen danach auch zurückgesetzt. Dies ist so, weil die Systemwiederherstellung immer nur die Veränderungen von Wiederherstellungspunkt zu Wiederherstellungspunkt sichert.

Windows XP erstellt bei der Installation neuer Treiber oder Programme mit *MSI-Installer* selbstständig einen Systempunkt. Bei allen anderen Programmen sollte dieser manuell vor der Installation erstellt werden.

Alle 24 Stunden wird ein Wiederherstellungspunkt automatisch erstellt. Das kann man in der *Registry* unter *HKEY_Local Machine\ SOFTWARE\ Microsoft\ WindowsNT\ CurrentVersion\ SystemRestore* mit dem Wert *RPGlobalInterval* ändern. Normalerweise ist er auf 86400 Sekunden voreingestellt, also 24 Stunden, man kann den Wert aber nach Belieben ändern.

Unter *Start ->Einstellungen-> Systemsteuerung-> System-> Systemwiederherstellung* kann man einstellen, welche Partitionen überwacht werden sollen bzw. ob die Systemwiederherstellung komplett deaktiviert werden soll. Unter Einstellungen kann man noch die maximale Größe bestimmen, die die Systemwiederherstellungspunkte verwenden dürfen. Im Regelfall überwacht man nur das Systemlaufwerk.

Zum Schluss noch ein Szenario zum Thema: Backup-Strategie und Krisenmanagement:

Grundlagen, Risiko- und Auswirkungsanalyse

- ✓ Bewerten Sie die Folgen des Datenausfalls für den Unternehmenserfolg
- ✓ Definieren Sie geschäftsrelevante Anforderungen an Notfallszenarien (Disaster Recovery)
- ✓ Potenzielle, materielle und immaterielle Verluste
- ✓ Welche Schäden auftreten können, Katastrophenszenarios
- ✓ Wie wichtig ein einheitliches, unternehmensweites Sicherheitskonzept ist
- ✓ Identifizieren Sie bedrohte Systeme
- ✓ Ermitteln Sie die Anforderungen an einen Wiederanlauf

Organisatorische Aspekte

- ✓ Beurteilen Sie Zeitspannen zur Umsetzung einer Notfallplanung
- ✓ Lohnt es sich, einen Dienstleister einzusetzen?
- ✓ Wie Sie eine Übersicht in Ihre Geschäftsfunktionen, Anwendungen und Daten bekommen
- ✓ Wer sich verantwortlich für die Organisation zeigen sollte
- ✓ Welche Impulse durch das Management gesetzt werden müssen

- ✓ Welche bewährten Vorgehensweisen existieren

Backup-Strategien

- ✓ Begrifflichkeiten
- ✓ Kaltes Backup, Warmes Backup, Heißes Backup
- ✓ Kommunikationsbeziehungen im heterogenen Umfeld
- ✓ Zentrale versus dezentrale Datenhaltung
- ✓ Server-Farmen versus dezentrale Server
- ✓ Ausgelagerte Datenträger versus Datenfernübertragung
- ✓ Was bringt zukünftig das Storage *Area Network* (SAN) an zusätzlicher Sicherheit?
- ✓ Arbeitsplatz-Backup

Technische Möglichkeiten und ihre Relevanz für die Notfallvorsorge

- ✓ Bandlaufwerke, RAID-Systeme
- ✓ Clustering-Lösungen, Fibre Channel, Remote Archive, Remote-Spiegelung

Physische Sicherheit

- ✓ Bewerten Sie Ihre Infrastruktur
- ✓ Erlangen Sie bereits durch richtigen äußeren Schutz erhöhte Sicherheit für Ihre Datenbestände
- ✓ Beurteilen Sie Schwachstellen

Einsatz eines Notfallplans und Notfallübungen

Notfallhandbuch

- ✓ Sorgen Sie durch Erstellung eines Notfallhandbuches vor
- ✓ Wie Sie richtige Dokumentationen erstellen, die Ihnen im Fall der Fälle Zeit und Geld sparen
- ✓ Wie Sie Prioritäten im Wert der Geschäftsfunktionen, Anwendungen und Daten setzen
- ✓ Welche Daten für wen relevant sind
- ✓ Wie Sie Handlungsanweisungen für den Wiederanlauf erstellen
- ✓ Planen Sie die Schritte von der Alarmierung im Notfall, über Notfallbetrieb und Schadensbeseitigung bis zur Wiederaufnahme des normalen Geschäftsbetriebes

Erstmaßnahmen im Schadensfall

- ✓ Welche Notfallüberbrückungsmaßnahmen existieren?
- ✓ Organisatorische und technische Abwicklung
- ✓ Wer sollte im Krisenstab sein und wie sind die Aufgaben verteilt?
- ✓ Wie Ihnen Dienstleister helfen können

Wiederanlaufplanung

- ✓ Not-/Alternativbetrieb
- ✓ Rückstandsaufholung
- ✓ Welche Impulse durch das Management gesetzt werden müssen
- ✓ Welche bewährten Vorgehensweisen existieren

Backup-Strategien

- ✓ Begrifflichkeiten
- ✓ Kaltes Backup, Warmes Backup, Heißes Backup
- ✓ Kommunikationsbeziehungen im heterogenen Umfeld
- ✓ Zentrale versus dezentrale Datenhaltung
- ✓ Server-Farmen versus dezentrale Server
- ✓ Ausgelagerte Datenträger versus Datenfernübertragung
- ✓ Was bringt zukünftig das *Storage Area Network* (SAN) an zusätzlicher Sicherheit?
- ✓ Arbeitsplatz-Backup

Technische Möglichkeiten und ihre Relevanz für die Notfallvorsorge

- ✓ Bandlaufwerke, RAID-Systeme
- ✓ Clustering-Lösungen, Fibre Channel, Remote Archive, Remote-Spiegelung

Physische Sicherheit

- ✓ Bewerten Sie Ihre Infrastruktur
- ✓ Erlangen Sie bereits durch richtigen äußeren Schutz erhöhte Sicherheit für Ihre Datenbestände
- ✓ Beurteilen Sie Schwachstellen

Einsatz eines Notfallplans und Notfallübungen

Notfallhandbuch

- ✓ Sorgen Sie durch Erstellung eines Notfallhandbuches vor
- ✓ Wie Sie richtige Dokumentationen erstellen, die Ihnen im Fall der Fälle Zeit und Geld sparen
- ✓ Wie Sie Prioritäten im Wert der Geschäftsfunktionen, Anwendungen und Daten setzen
- ✓ Welche Daten für wen relevant sind
- ✓ Wie Sie Handlungsanweisungen für den Wiederanlauf erstellen
- ✓ Planen Sie die Schritte von der Alarmierung im Notfall, über Notfallbetrieb und Schadensbeseitigung bis zur Wiederaufnahme des normalen Geschäftsbetriebes

Erstmaßnahmen im Schadensfall

- ✓ Welche Notfallüberbrückungsmaßnahmen existieren?
- ✓ Organisatorische und technische Abwicklung
- ✓ Wer sollte im Krisenstab sein und wie sind die Aufgaben verteilt?
- ✓ Wie Ihnen Dienstleister helfen können

Wiederanlaufplanung

- ✓ Not-/Alternativbetrieb
- ✓ Rückstandsaufholung
- ✓ Wiederaufnahme des gewohnten Geschäftsbetriebs
- ✓ Fallbeispiele

Üben Sie den Notfall

- ✓ Wie Sie die Katastrophe üben können, um im Ernstfall gut vorbereitet zu sein
- ✓ In welchem Rhythmus der Katastrophenfall geübt werden sollte
- ✓ Wer sich für die Durchführung verantwortlich zeigen sollte
- ✓ Wie Sie die Ergebnisse messen und bewerten

Krisenmanagement und Krisenstab in der Praxis

- ✓ Wie erkennt man eine Krise?
- ✓ Wer oder was löste eine Krise aus?
- ✓ Welche Kommunikations- und Organisationsprinzipien werden im Krisenfall angewendet?
- ✓ Was sind die Ziele der Krisenbewältigung?
- ✓ Woher bezieht der Krisenstab seine Informationen?
- ✓ Wie kommuniziert das Unternehmen in der Krise nach außen?

Krisenmanagement

- ✓ Überblick: Was für die Bewältigung von Krisen wichtig ist
- ✓ Anwendungsbereich des Krisenmanagements
- ✓ Abgrenzungen des Krisenmanagements zum Notfall- und Katastrophenfallmanagement
- ✓ Die Risikoanalyse: Kernstück des vorbereitenden Krisenmanagements
- ✓ Schnittstellen zum Business- und IT-Recovery
- ✓ Aufbau und Aufgaben des IT-Notfallteams
- ✓ Auslöser einer Krise und die Auslösung des Krisenmanagements
- ✓ Eskalationsstufen und Rolling Disaster

Organisation und Zusammensetzung des Krisenstabs

- ✓ Welche Personen und Funktionen sollten Mitglieder im Krisenstab sein?
- ✓ Wie sehen wirksame Organisationsprinzipien für den Krisenstab aus?
- ✓ Welche Entscheidungsbefugnisse und Kompetenzen hat der Krisenstab?
- ✓ Anforderungen an die Qualifikation der Mitglieder
- ✓ Die Einberufung des Krisenstabs
- ✓ Der Umgang mit den Medien
- ✓ Die Information der Mitarbeiter

Die funktionierende Krisenstabszentrale(n)

- ✓ Lokationen: Welche Anforderungen eine Krisenstabzentrale erfüllen muss
- ✓ Vorbereitung und Einrichtung der Krisenstabszentrale
- ✓ Wie Sie die Erreichbarkeit des Krisenstabs sicherstellen

Dokumentation: Die Basis für die Arbeit des Krisenstabs

- ✓ Erstellen und Pflegen des Krisenmanagementleitfadens
- ✓ Technische Unterstützung
- ✓ Die Alarmierung des Krisenstabs
- ✓ Der Pocket-Guide für Krisenfälle

Spezielle Situationen die Krisenmanagement erfordern

- ✓ Krisenprävention
- ✓ Geiselnahme und Entführung
- ✓ Bombendrohung
- ✓ Feuer Wasser
- ✓ Betriebsschließungen
- ✓ Produktschutz

Inkraftsetzen des Krisenmanagements

- ✓ Nach welchem Verfahren sollte ein Krisenmanagement genehmigt werden?
- ✓ Veröffentlichung: Wer stellt das Vorliegen einer Krise fest und kommuniziert es?
- ✓ Wie kann eine Schulung für Krisenfälle aussehen?
- ✓ Binnenmarketing
- ✓ Technische Hilfsmittel

Krisenmanagementübung

- ✓ Die Vorbereitung der Übung
- ✓ Welche Ziele wollen Sie durch die Übung erreichen?
- ✓ Umfang der Krisenmanagementübung
- ✓ Auswertung und Nachbereitung