

# *Sicherung einer Festplattenpartition*

mit

**Paragon DriveBackup 9 Express**

in 19 Schritten

# Inhaltsverzeichnis

- [1. Vorwort](#)
- [2. Programmbeschaffung und Installation](#)
- [3. Festplatte reinigen](#)
- [4. Festplatte defragmentieren](#)
- [5. Erhöhung der Sicherheit](#)
- [6. Beschleunigung und Tuning](#)
- [7. DVD-RWs zum Brennen vorbereiten](#)
- [8. Rettungs-CD brennen](#)
- [9. Kurztest der Rettungs-CD](#)
- [10. Menüführung in DriveBackup](#)
- [11. Backup auf DVD erstellen](#)
- [12. Qualitätsprüfung des Backup](#)
- [13. Restore auf verkleinerter Partition C:](#)
- [14. Ein wenig „trockene Theorie“](#)
- [15. Weitere Partitionen erstellen](#)
- [16. Festplatte endgültig einrichten](#)
- [17. Profil des Firefox verschieben](#)
- [18. Neues Backup auf der Festplatte erstellen](#)
- [19. Restore von Festplatte](#)
- [20. Pflege des Image](#)
- [21. Nachwort](#)

## **Achtung, wichtigster Hinweis:**

Backups, welche auf diese oder ähnliche Art und Weise hergestellt werden, sind keine Handelsware. Sie dürfen weder gegen Bezahlung noch kostenlos weitergegeben und nur im eigenen Bedarf, auf dem gleichem PC verwendet werden. Grundsätzlich gelten die Rechtsvorschriften, welche allen verwendeten und zu sichernden Programmen beigelegt sind.

Autor: Manfred Fiebig

Homepage: <http://www.hinterwaeldlers-home.de/>

Kontakt : [manfred\\_fiebig@arcor.de](mailto:manfred_fiebig@arcor.de)

# Vorwort

Dieses Tutorial ist vergleichbar mit Freeware und kann, soweit es unverändert bleibt und die Urheberrechte nicht verletzt werden, jederzeit vervielfältigt und an Dritte weitergegeben werden. Sollte dieser oder jene User grundsätzliche Fehler im Wortlaut oder Sachverhalt finden, dann bitte ich Ihn, diese mir in Verbindung mit einem Korrekturvorschlag zu übermitteln. Bitte lasst es mich wissen.

Die Gefahren aus dem Internet sind kaum noch überschaubar. Eben war unser PC noch völlig in Ordnung und nach dem Besuch einer scheinbar harmlosen Website ist er außer Rand und Band geraten. Dieses vor einigen Jahren noch unvorstellbare Horrorszenario ist heute hoch aktuell. Reichten damals ein monatlich aktualisierter Virens Scanner aus, so bedeutet dies unter den heutigen Bedingungen die Kompromittierung unseres Systems innerhalb weniger Minuten.

Bedenkt dabei: Die Kompromittierung ist unter den Bedingungen des DSL 1000 nach Ausführung der Malware in weniger als 20 Sekunden vollzogen. Wer glaubt einen sicheren Scanner zu besitzen, sollte sich bei <http://virusscan.jotti.org/de/> vom Gegenteil überzeugen. Nur Malware die schon Monate im Umlauf ist, wird gefunden. Aktuelle nicht.

Ein gut konfiguriertes System ist Pflicht und ein regelmäßiges Sicherheitsbackup ist unter diesen Bedingungen unbedingt notwendig. Ausgerechnet beim Sicherheitsbackup wird von vielen Usern gespart. Einesteils, weil die angebotene Software bisher meist ungeeignet und wenn doch, dann sehr umständlich zu bedienen war. Anderenteils hat Microsoft besonders bei den neueren Betriebssystemen (2000, XP, Vista) sein eigenes Süppchen gekocht. Ein Backup wurde zugunsten der Systemwiederherstellung sträflich vernachlässigt. Mit diesem Tool hat so mancher schon sein persönliches Waterloo erlebt.

Hat dann ein User wirklich mal versucht, mit einem konventionell erstellten Backup die Systemdateien etc. wieder herzustellen, war ein Bluescreen vorprogrammiert. Aus heutiger Sicht müssen wir sagen: Zwar hat MS in den vergangenen Jahren versucht den Forderungen der Anwender nach mehr Sicherheit gerecht zu werden, jedoch wurde das Pferd am falschen Ende aufgezäumt.

Dies war der Ansatzpunkt renommierter Unternehmen und Freizeitprogrammierer ein neues System des Backup/Restore zu schaffen, das den heutigen Forderungen an unser Sicherheitsbedürfnis gerecht wird. Und was hat der Herr BG alles schon angestellt, um ausgerechnet dies zu verhindern. Hobby-Programmierern wurde es sogar per Gerichtsbeschluss untersagt solche Lösungen anzubieten, weil diese angeblich die Rechte Microsoft's verletzen. Ich spreche in erster Linie von Bart Lagerweij's **PEBuilder** in seiner ursprünglichen Fassung. Ausgerechnet MS fühlte sich in seinen Rechten beschnitten, dabei brauchen wir nur mal in der Historie von MS blättern... Tuts auch.

Nur große Software-Unternehmen hatten dann die Kapazität und das Know How eigener, auch unter XP funktionsfähige Lösungen anzubieten. Marktführer waren bislang Symantec und Acronis. Etwas im Schatten befand sich Paragon mit Drive Backup bzw. Festplattenmanager. Mit dem kostenlosen neuen **Drive Backup 9 Express** verteilt Paragon ein Tool, das den Vorstellungen eines ONU **OttoNormalUser** von einem Programm dieser Kategorie weitestgehend entspricht. Drive Backup 9 Express ist überdurchschnittlich schnell und äußerst einfach zu bedienen. Zwei Hindernisse stehen der allgemeinen Anwendung von ONU entgegen, eine in computerenglisch gehaltene

Menüführung und spartanische Hilfedatei in englischer Sprache.

Der ONU, welcher der Werbung seines Lebensmitteldiscounters zum Kauf eines PC erlegen ist, sieht sich hilflos unüberwindbaren Problemen gegenüber. Dabei ist alles so einfach. Ich werde es in wenigen Schritten ausführlich erklären und versichere Euch: Wer den einmaligen Zeitaufwand einiger Stunden zur Vorbereitung nicht gescheut hat und das erste Test-Restore probierte, wird dieses Tool nicht mehr missen wollen.

Einige Leser dieses Tutorials werden mir verzeihen, das ich in der Beschreibung davon aus gehe, das Euer PC nur eine Partition, also nur das HD-Laufwerk C: besitzt. Dies ist oft der Auslieferungszustand eines PC der unteren Preisklasse. Speziellen Fachkenntnisse des Anwenders werden nicht vorausgesetzt. Darum sind erstes Backup, erstes Restore und deren Erläuterung besonders umfangreich ausgefallen. Handelt der ONU genau so wie hier beschrieben, wird ein späteres Backup und Restore nur noch das Werk einiger Minuten sein.

Trotz großer Bemühungen war es mir nicht möglich, in jedem Fall exakte Screenshots beizufügen, denn ich besitze nur einen PC und verwende schon seit vielen Jahren mehrere Partitionen. Ich glaube jedoch mit meinen Bildern immer den Kern der Sache getroffen zu haben. Das Tutorial ist so geschrieben, dass der Newcomer bei jedem Schritt die dazu gehörende Seite des Tutorials auf dem Desktop öffnen kann. Leider ist dies während des Step „Restore auf verkleinerter Partition C:“ nicht möglich und empfehle darum bei eventuellen Unsicherheiten diesen Schritt zu drucken oder in Stichpunkten abzuschreiben.

**Wichtig:**

Wer mit Drive Backup ein Backup erstellt, sollte während dieser Zeit den Bildschirmschoner und die Energieverwaltung unter

*Desktop-Rechtsklick -Eigenschaften/Bildschirmschoner/Button [Energieverwaltung]*

grundsätzlich auf "Aus" bzw. auf "Nie" schalten. Ansonsten kann das Archiv beim automatischen Einschalten des Screensavers Fehler erhalten und nicht mehr gelesen werden können. (Nobody is perfekt).

# Programmbeschaffung und Installation

Als erstes benötigen wir natürlich das Programm **Paragon Drive Backup 9 Express**. Wir erhalten es auf der US-amerikanischen Homepage von Paragon und bislang sonst nirgends. Wir rufen die Page mit

[http://www.paragon-software.com/downloads/free\\_downloads.html](http://www.paragon-software.com/downloads/free_downloads.html)

auf und wählen den weiterführenden Link „Download for FREE“. Dort müssen wir uns zwischen einer 32 und 64 Bit-Architektur des Betriebssystems entscheiden. Wer dies nicht auf Anhieb sagen kann geht auf dem Desktop in Arbeitsplatz und wählt nach einem Rechtsklick die Eigenschaften aus. Nur wenn dort ausdrücklich auf ein 64-Bit System verwiesen wird, ist es auch eines.

Nach dem Download wird das Programm installiert. Am Anfang des Setup werden wir zur Eingabe des Key aufgefordert und können zu dessen Beschaffung den Button benutzen. Es dauerte keine 2 Minuten und er befand sich in meiner Mailbox. In diesem Zusammenhang: Ich habe mich bei Paragon schon X-Mal registriert und in dessen Folge noch niemals Spam erhalten, welcher auf diesen Hersteller zurückzuführen ist. Andere sind weniger zimperlich. Die Registrierungsdaten schreiben wir uns auch sofort auf, Damit sie nicht mehr verloren gehen. Bei mir steht dann so was immer auf der Inhaltsangabe der CD und wird gleich mit gebrannt.

Weil wir einmal dabei sind, wir brauchen noch mehr kleine Freeware-Programme:

WinDirStat deutsch von	<a href="http://www.windirstat.info/">http://www.windirstat.info/</a>
FreeCommander von	<a href="http://www.freecommander.com/de/index.htm">http://www.freecommander.com/de/index.htm</a>
CCleaner von	<a href="http://www.ccleaner.com/">http://www.ccleaner.com/</a>
Script zur Erhöhung der Sicherheit	<a href="http://www.ntsvcfg.de/">http://www.ntsvcfg.de/</a>
Revo Uninstaller von	<a href="http://www.revouninstaller.com/">http://www.revouninstaller.com/</a>
Autoruns, ProcessExplorer, TcpView, RootkitRevealer von	<a href="http://www.sysinternals.com">http://www.sysinternals.com</a>

Einige von Euch werden nun sagen: „Hah, ich viel habe bessere und tollere Software.“ Wir brauchen aber keine anderen und die Tools von Sysinternals sind viel besser zur Erkennung von Malware geeignet als die teuersten Internet-Securitys. Ihr kommt schon auch noch dahinter, mancher allerdings nie.

# Festplatte reinigen

Zunächst untersuchen wir mit Autoruns von Sysinternals unser System. Sollten nämlich schon jetzt Autostarts unerwünschte Programme gefunden werden, erübrigt sich das Säubern der Festplatte und installieren Windows gleich neu. Tun wir es nicht, wäre es ein nicht mehr kalkulierbares Risiko, das bis zum Verschrotten des PCs auf der HDD mitgeschleppt würde.

Wir starten Autoruns und schalten im Menüpunkt „Options“ die Eigenschaft „Hide Microsoft Entrys“ ein. Nach einem Programmneustart wird die Anzeige sofort viel übersichtlicher. Das erste Register *Everything* dient eigentlich nur der Dokumentation und einem späteren Vergleich. Nun muss eine aktive Verbindung zum Internet vorhanden sein und wir suchen alle anderen Register nach seltsamen oder undokumentierten Einträgen. Haben wir einen gefunden, markieren wir ihn und wählen nach einem Klick mit der rechten Maustaste *Search Online*.... Innerhalb weniger Sekunden zeigt euch Google alle Treffer im Internet, die mit der Datei in Verbindung gebracht wurden.

Da die Treffer überwiegend englisch sind, bleibt euch nichts weiteres übrig, als sie ein wenig zu interpretieren. War es nur allgemeines Gewäsch, ist es gut. Nur wenn in den Forum-Threads diese Dateien als Malware deklariert ist oder wenn nur ganz wenige Treffer existieren, ist von einer Kompromittierung des Systems auszugehen. In diesem Fall ist nach dieser Anleitung <http://www.pctipp.ch/forum/showthread.php?t=519> zu verfahren, auch wenn es mir sehr Leid tut.

Wichtig: Zu jeder in Autoruns angezeigten Datei gibt es Treffer bei Google. Es sei denn, diese Datei ist nagelneu und damit unbekannt. Dann herrscht höchste Gefahr.

Ergab die Prüfung keine Einträge, können wir mit einer Grundsäuberung beginnen. Als Erstes tun wir das, was eigentlich nach ca. 30-40 Betriebsstunden fällig ist. Auch dann, wenn wir zeitlich unter Druck stehen. Unbeschreiblich, wie viel Datenmüll sich auf einer Festplatte befinden kann. Zur Beräumung benutzen wir eines der besten deutschsprachigen Freeware-Tools. Es ist **CCleaner**. Er ist übersichtlich und schnell.

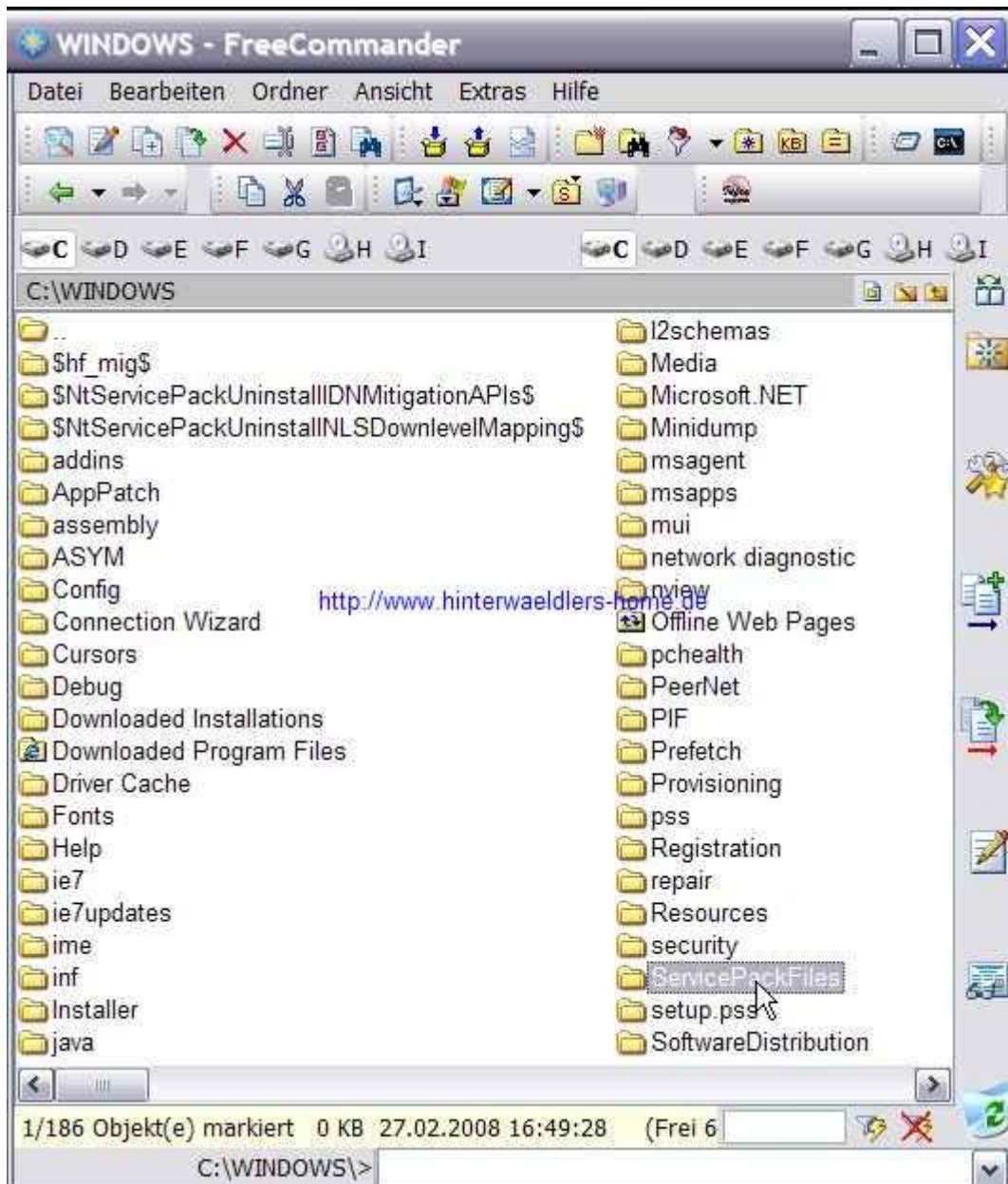
Wer es noch niemals benutzte, wird anfangs etwas über die vielfältigen Optionen erstaunt sein und auch darüber, was alles überflüssig ist und problemlos entfernt werden kann. Nehmt euch die Zeit und geht vor dem ersten Start die paar Menüpunkte durch, aktiviert alles. Nicht ängstlich sein, es wird tatsächlich nur Müll entsorgt. Windows ist ein unverbesserlicher notorisch Müllsammler. Eure Festplatte atmet im Anschluss sichtbar auf und verhält sich ähnlich wie jemand, der nach Beendigung einer schweren körperlichen Arbeit unter der Dusche gestanden hat.

Im weiteren Verlauf entsorgen wir mit dem **Revo Uninstaller** alle längst vergessenen Programme, die ihr zwar mal installiert aber noch nie wirklich gebraucht habt. Dazu zählen auch solche, welche vom Anfang an auf der Festplatte waren und ihr noch nie begriffen habt, wozu sie überhaupt nutze sind. Trennt euch davon, der Uninstaller macht es selbst in seiner default-Einstellung sehr zuverlässig. Windowseigene Programmbestandteile werden kaum angezeigt und wenn doch, sind sie bekannt. Updates, welche mit KB... beginnen, tasten wir auch nicht an.

Die folgende Reinigung des Systems wird von keinem bekannten Fremdprogramm übernommen. Dazu klicken wir mit der rechten Maustaste im Ordner "Arbeitsplatz" auf die

Festplatte C:.. Im sich jetzt öffnenden Kontextmenü wird der Punkt "*Eigenschaften*" gewählt. Hier benutzen wir den Button [**Bereinigen...**]. Hat XP allen Müll gefunden (den **nur das System** verwaltet!), werden im sich jetzt zeigenden Fenster alle Option aktiviert. Auch dabei nicht ängstlich werden. Es handelt sich wirklich nur um Datenmüll, welcher niemals mehr gebraucht wird.

Im weiteren Verlauf klicken wir sofort auf die Registerkarte [*Weitere Optionen*] und dort im Abschnitt **Systemwiederherstellung** auf den Button [**Bereinigen...** ]. Die Sicherheitsabfrage wird mit [**Ja** ] bestätigt. Die nun folgende Bereinigung der Festplatte wird mit [**Ok** ] eingeleitet. Wer dies zum ersten Mal tut und jetzt das Fenster mit der Tortengrafik im Blickfeld hat, wird mir bestätigen: Diese kleine Mühe hat sich gelohnt.



Jetzt treten wir in eine weitere Phase der Grundreinigung und benutzen einen richtigen Dateimanager. Ich gab oben den FreeCommander an. Wer das erste Mal damit arbeitet, wird über seine Funktionsvielfalt erstaunt sein. Übt ein wenig mit der Navigation und lest die Hilfedatei. Wichtig ist die Einstellung im Menü-Extras-Ansicht *Versteckte Dateien anzeigen* und *Systemdateien anzeigen*. Wir gehen zuerst nach

*Dokumente und Einstellungen\<Username>\Lokale Einstellungen\temp\*

und löschen dessen Inhalt. Keine Angst, vom Löschen solchen Unfugs geht Euer PC nicht kaputt. Eventuell nicht löschbare Dateien sind von Programmen zur Bearbeitung geöffnet und brauchen euch nicht beunruhigen.

Inf unserer Tour gehen wir nach [C:\Windows](#) und entfernen alle Verzeichnisse, die mit einem \$-Zeichen beginnen. Darin befinden sich alle Backup-Dateien der der kürzlich oder auch vor langer Zeit installierten Sicherheitspatches von MS\$. Falls euer System nach den Patches fehlerfrei läuft, ist dort der Schnee der vergangenen Jahre gelagert. Es ist kaum anzunehmen, das ihr ganz urplötzlich aus heiteren Himmel einen Patch von vor zwei Jahren wieder rückgängig machen wollt.

Weiterhin fallen dort vorhandene Verzeichnisse des IE 7 unserer Radikalkur zum Opfer. Sie beinhalten die ursprünglichen Setupdateien, deren Konfigurationen und die späteren Patches. IE7 ist längst fest installiert, nur MS kümmert sich nicht mehr um sie.

Nun das letzte Hammerverzeichnis für User, die XP schon seit vielen Jahren besitzen. Es ist das Verzeichnis `..\ServicePackFiles\.` Unbeschreiblich, was sich darin befinden kann. Es sind alle von den Servicepacks vor vielen Jahren ausgetauschten und dort aufbewahrten Dateien. Die braucht kein Mensch mehr, noch weniger euer System. Also weg damit oder wusstet ihr, wie man ein installiertes SP1 wieder entfernt? Wer bis jetzt noch Bedenken hatte, den möchte sich daran erinnern, wie groß sein Windows mit allen Unterverzeichnissen war, als ihr es das erste Mal im vollem Bewusstsein betrachtet habt und in der Folge enttäuscht wurdet, weil es aufquoll wie ein Hefeklos. Vordem funktionierte es aber auch. Nun haben wir diesen Zustand fast wieder erreicht.

Zum Schluss installieren wir WinDirStat und sehen uns den statistischen Platzbedarf aller Dateien grafisch an. Die Rechtecke symbolisieren den relativen Platzbedarf und ihre Farbe repräsentiert den Dateityp. Finden wir ein Rechteck auffälliger Größe, gehen wir mit dem Mauszeiger darauf und erfahren in der Statuszeile den Namen und Speicherort. Oft bleiben diese als Überreste verunglückter Brennversuche oder abgebrochene Videokonvertierungen irgendwo übrig. Manchmal sind es auch längst verschollene Downloads. Weg damit, ihr habt sie bis heute nicht gebraucht.

Solltet ihr auf diesem Weg Dateien finden, welche von euch noch gebraucht werden, zum Beispiel Movies, MP3s, eure Bildersammlung oder gar eventuelle Setupdateien der von euch verwendeten Programme, dann sichert diese auf wiederbeschreibbaren CDs oder DVDs. Sie sind dort eh besser aufgehoben als in den Tiefen eurer Festplatte. Solche Folter wie in „Eigene Dateien“ erscheinen im ersten Moment sehr praktisch, werden aber bei einem Restore des Image komplett überschrieben und sind damit auf der C: sinnfrei. Zudem kann deren Inhalt kaum effektiv verwaltet werden. Erinnert euch an die Menge Müll, die ihr schon beseitigt habt. Jedes aktuelle Programm erlaubt es in seinen Einstellungen, andere und leichter auffindbare Arbeits- und temp-Verzeichnisse auf anderen Partitionen dauerhaft zu benutzen.

Größere Spiele, von denen ihr eine Installationsdisk besitzt (das sollte man eigentlich ;-), werden ebenfalls mit **Revo Uninstaller** deinstalliert und später neu installiert. Sie vergrößern nur unnötig die Images. Es gibt noch einen anderen Grund: Würden sie auf der Festplatte verbleiben und mit ins Backup genommen, könntet ihr selbst in einigen Jahren noch, das längst fertig gespielte Spiel nach einem Restore wieder auf der C: vorfinden. Das würde zwar euch erheitern, aber kaum wirklich sinnvoll sein.

## Festplatte defragmentieren

Habt Ihr Euch den Anfangsbetrag des Festplatteninhaltes mal aufgeschrieben und mit dem jetzigen Inhalt verglichen? Und funktioniert Euer PC noch immer? Na also. Jetzt haben wir den Inhalt der Festplatte soweit reduziert, dass eine Defragmentierung sich eher lohnt.

Es befinden sich entschieden weniger Dateien darauf. Zum Defrag klicken wir wieder im Ordner **Arbeitsplatz** mit der rechten Maustaste auf die Festplatte C: und wählen den Menüpunkt **Eigenschaften**. Weil wir gerade hier sind - seht Euch mal in der obersten Editorzeile den Namen eurer Festplatte an. Zufrieden damit? Herr M\$ ist es jedenfalls, er hat ihn ja ungefragt vergeben. Na gut, wir schreiben mal ganz einfach und noch beeindruckt vom Step 2 "*Microsoft's Müllhalde*" hinein und ab sofort heißt das Laufwerk so. Auch nicht gut? Dann lasst Euch mal was anderes einfallen.

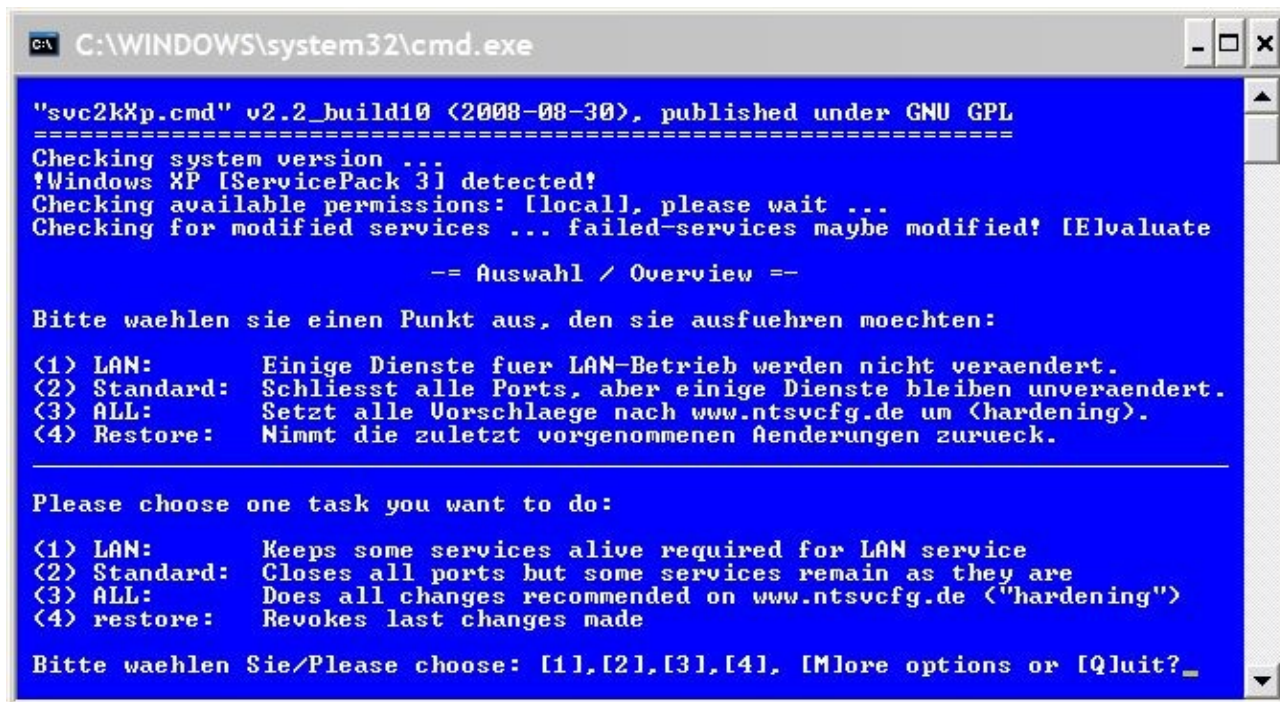
Ist die Namensverleihung erledigt wählt ihr das Register **Extras**. Hier finden ihr den Aufruf zum Defragmentieren der Festplatte. Glaubt mir, wer dies das erste Mal durchführt nimmt an, das Tool funktioniere nicht. Moderatoren einschlägiger Foren können ein Lied davon singen. Ihr müsst wirklich nur genügend Geduld aufbringen. Stellt Euch dabei mal folgendes vor: Während dieses Vorganges werden mehrere Gigabyte Daten in eine völlig andere Anordnung gebracht und dutzende Systemdateien, die selten gebraucht werden (so genannte "alte" Dateien), mit dem Windows-Komprimierungstool zusammen gestaucht und ebenfalls neu angeordnet. Das ist nicht so schnell erledigt, wie sich dies mancher vorstellt.

In diesem Zusammenhang muss ich nochmal auf die Prefetchdateien im zugehörigen Windows-Unterverzeichnis zurückkommen. In diesen Dateien notiert Windows wie oft und wann das letzte Mal die jeweilige ausführbare Datei oder Treiber aufgerufen wurde. Daraus errechnet das Windows-Defrag (und kein anderes Tool) die optimale Anordnung der Datei auf der Festplatte und verschiebt während des Defragmentieren die Dateien an diese optimale Adresse. Prefetch dient also der Optimierung der Geschwindigkeit des Systems. Anders lautende Argumente jeglicher Art sind dümmliches Geschwätz einiger Wichtigtuere und Besserwisser. Eventuelle Lücken in der Anordnung der Dateien auf der Festplatte sind bewusst eingefügt und bieten den Platz für temporäre Dateien der Programme. Diese können dann so auf der Festplatte abgelegt werden, dass der Actuatorarm mit dem Schreib-Lesekopf sich nicht mehr als nötig bewegen muss. Diese Lücken dienen damit der Erhöhung der Lebensdauer der Festplatte und haben nichts mit der oft von anderen Herstellern angeführten Unfähigkeit Mickysofts zu tun. In diesem Fall ist das Gegenteil der Fall. Auch in anderen Dateisystemen sind solche Lücken durchaus üblich. Ist die Defragmentierung erledigt, beenden wir den PC und starten neu.

Übrigens hat MS ab SP2 für XP an dieser Stelle eine kleine Änderung vorgenommen, denn seit dieser Zeit defragmentiert das System die Startpartition automatisch, falls es mal mehrere Minuten nichts zu tun hat. Es ist also kein Fehler, wenn euer XP während einer Kaffeepause auf einmal anfängt, die Festplatte zu defragmentieren. Wer aber auf einen dieser seltsamen Tweaker vertraut und diese Funktion abgeschaltet hat, ist wohl selbst schuld. Einklicktools schalten gar ohne euch zu fragen ab oder deren Fragestellung ist so gehalten, dass ihr deren Inhalt nicht versteht.

## Erhöhung der Sicherheit

Ihr geht nicht fehl, wenn hier jetzt etwas Besonderes beschrieben wird, denn seit Ende 2004 ist bekannt, dass Personal Firewalls nicht nur so gut wie nutzlos sind, sondern selbst eine zusätzliche Fläche für Angriffe aus dem Internet oder von schon installierter Malware bilden. Mit anderen Worten: In Zeiten, in welchen Sober, Beagle & Co. die dominierende Malware sind, hilft nur noch eine sinnvolle Konfiguration des Systems. Diese ist so zu gestalten, dass alle unnötigen Dienste beendet und damit gleichzeitig auch alle zum Internet geöffneten zusätzlichen Ports geschlossen sind.



```
C:\WINDOWS\system32\cmd.exe

"svc2kxp.cmd" v2.2_build10 (2008-08-30), published under GNU GPL
=====
Checking system version ...
!Windows XP [ServicePack 3] detected!
Checking available permissions: [local], please wait ...
Checking for modified services ... failed-services maybe modified! [E]valuate

      == Auswahl / Overview ==

Bitte waehlen sie einen Punkt aus, den sie ausfuehren moechten:

(1) LAN:      Einige Dienste fuer LAN-Betrieb werden nicht veraendert.
(2) Standard: Schliesst alle Ports, aber einige Dienste bleiben unveraendert.
(3) ALL:      Setzt alle Vorschlaege nach www.ntsvcfg.de um (hardening).
(4) Restore:  Nimmt die zuletzt vorgenommenen Aenderungen zurueck.

-----
Please choose one task you want to do:

(1) LAN:      Keeps some services alive required for LAN service
(2) Standard: Closes all ports but some services remain as they are
(3) ALL:      Does all changes recommended on www.ntsvcfg.de ("hardening")
(4) restore:  Revokes last changes made

Bitte waehlen Sie/Please choose: [1],[2],[3],[4], [M]ore options or [Q]uit?_
```

Wie ihr seht, hat dieser kleine Konfigurationsscript `svc2kxp.cmd` von <http://www.ntsvcfg.de/> nur vier Möglichkeiten. Für Otto Normalo sind die beiden ersten Möglichkeiten von Bedeutung. Dieses kleine Werkzeug ist OpenSource und kann damit von jedem Anwender im Quelltext nach geprüft werden. Bitte lest auch den Abschnitt „Bekanntes Probleme“. Für den Heimanwender sind die Ausführungen in der Regel bedeutungslos. Ihr solltet aber wissen, dass es sie gibt und wie man sie eventuell abstellen kann. Sollte wirklich Müll entstanden sein, könnt ihr mit der vierten Option die Einstellungen wieder rückgängig machen.

Wichtig sind noch diese Bemerkungen:

Dieser Script schaltet alle Funktionen des Sicherheitscenters vom WindowsXP SP2 und damit auch das automatische Update ab. Um nun monatlich die Fixes und Patches zu installieren, sollte die ursprüngliche Defaultkonfiguration wieder hergestellt werden (Option 4: Restore). Die Anwendung anderer Tweaker sollten tunlichst vermieden werden. Sie richten meist mehr Schaden an, als sie Nutzen besitzen. Mehr über Tweaker und ihre meist sehr seltsamen Eigenschaften findet ihr bei <http://www.derfisch.de/node/129> Gleich im voraus: Der Betreiber dieser Page mit Forum ist beruflich Administrator eines großen Firmennetzes in der Nähe von Frankfurt/Main und muss sich in dieser Eigenschaft täglich der Not gehorchend mit diesen Problemen beschäftigen.

Einige Anwender lehnen `svc2kxp.cmd` "Dienste abschalten" mit der Begründung ab, dass

damit die Funktionalität ihres Systems eingeschränkt würde. Das Argument musste ich dreimal lesen, damit ich einmal den ganzen Wortlaut verstand. Wenn ich zum Beispiel mit der Konfiguration 3 "**All**" zu Microsoft gehe, um meine Patches herunter zu laden, erhalte ich eine Fehlermeldung und ich weiß auch warum. Was hindert mich jetzt daran, mit zwei-drei Mausklicks und einem Systemneustart diese Konfiguration so zurück zu stellen, das ein Update problemlos gelingt? Fehlermeldungen, die Personal-Firewalls am laufenden Band produzieren, sind meist schwieriger zu deuten.

In diesem Zusammenhang habe ich vor einiger Zeit im Forum von EXELBONSAI in <http://tinyurl.com/8cgglc> eine Anleitung für ältere Menschen mit dem Titel "**Mit WindowsXP sicher ins Internet**" veröffentlicht. Es wurde so geschrieben das auch Senioren, die plötzlich ihr neues Hobby im Computer entdeckten, problemlos ihren PC beherrschen. Das soll aber nicht bedeuten, das Jüngere sie nicht lesen können. Der Inhalt wurde nach der Erstellung von einigen Mitgliedern des CCC geprüft. Ihre Hinweise sind eingearbeitet. Verzeiht mir, wenn der Inhalt nicht immer dem aktuellsten Stand der Technik und den neuesten Erkenntnisse entspricht. Grundsätzlich Falsches steht mit Sicherheit nicht drin.

# Beschleunigung und Tuning

Viele Anwender sind, geschürt von einer manchmal nicht ganz seriösen Fachpresse, verunsichert und zur Überzeugung gelangt, ihr Windows müsse zwingend tiefer gelegt werden. Dann beschaffen sie sich aus den verschiedensten, oft nicht einmal vertrauenswürdigen Quellen solche Tweaker wie **MagicTweak**, **TweakNow**, **PowerPack**, **xpTuner**, **XPAntiSpy**, **TuneUp**, **BootVis**, **TuneXP** und andere. Schon ihr Name suggeriert Überheblichkeit. Ich gestehe auch auf dieser Welle mal geritten zu sein, bis ich eines Tages urplötzlich ein paar ganz wesentliche Dinge feststellte:

1. Trotz allem Tunens ist mein System zwar nicht schneller aber instabiler geworden
2. Richtige und falsche Einstellungen summierten sich Grundsätzlich zu nicht mehr behebbaren Fehlern
3. Irgendwann habe ich vergessen, welche Einstellung ich mit welchem Tool gemacht habe
4. BootVis hat mir ein Tracing installiert, welches ich nur noch mit einem selbst geschriebenen Script beenden konnte

Kommt euch das bekannt vor? Also habe ich mich mit der Materie näher befasst und kam zu einem erstaunlichem Ergebnis. Diese Erfahrungen fasste ich in einem eigenen kleinen "**Hinterwäldlers SuperTweaker**" zusammen. Dieses Tool kann bei EXELBONSAI <http://tinyurl.com/c9p8f> heruntergeladen werden. Mittlerweile gibt es in diesem Forum sogar ein Update: <http://tinyurl.com/cpnre>. Völlig kritiklos wurde der Tweaker nicht hingenommen und einige wenige Anwender glaubten gar, ich würde sie verschaukeln und waren ernsthaft beleidigt. Das kann man im zugehörigen Thread herauslesen.

Andererseits, der Zähler für die Downloads spricht für dieses kleine unbekanntes Forum eine deutliche Sprache. Fest steht: So viele Optionen wie dieses Werkzeug bietet, besitzt kein anderes. Und was noch wichtiger ist, es verändert die Einstellungen genau dort, wo es von Microsoft vorgesehen ist, damit bleibt die Stabilität des Systems gewahrt. Alle Einstellungen sind reproduzierbar. Tritt jetzt ein Fehler auf, kann jeder Laie oder Fachmann die Einstellungen auch **ohne** "Hinterwäldlers SuperTweaker" wieder rückgängig machen.

## DVD-RWs zum Brennen vorbereiten

Jetzt haben wir unsere Festplatte in guten Verfassung und kontrollieren noch einmal alle von uns durchgeführten Verbesserungen. Bedenkt dabei, jeder überflüssige Müll, jede falsche Option und jedes defekte Programm wird, so oft wir auch unser Festplatten-Backup auf der HD restaurieren, immer wieder erscheinen.

Welche Datenträger sollten wir als Backupmedium nun benutzen? In früheren Anleitungen beschrieb ich eine sehr umständliches Prüfungsverfahren für CD-RWs. Diese Prüfung machte sich auf Grund ihrer vielen Fehler erforderlich. Ich konnte nach diesen Verfahren ca. 50% der Scheiben selbst teurer Markenherstellern als für diese Zwecke ungeeignet aussortieren. Inzwischen sind selbst die preiswertesten DVD-RW aus dem Supermarkt um vieles besser als die meisten anderen optischen Datenträger. Sie werden nur noch von der DVD-RAM übertroffen. Auch diese sind erschwinglich, können aber nur mit einem zusätzlichen Treiber effektiv beschrieben werden. Also benutzen wir DVD-RW aus dem Edeka für 3,99 je 5-er Pack.

Um eine Qualitätsprüfung kommen wir nicht herum. Diese kann aber vor dem ersten Restore mit Hilfe der Möglichkeit der Verifizierung durch DriveBackup Express gemacht werden und wird dort in diesem Zusammenhang beschrieben.

Wir müssen aber noch die Frage klären, wie viel DVD-RWs wir benötigen. Da unser kleines *Drive-Backup 9 Express* Archive nicht komprimieren kann, gehen wir von dieser Faustregel aus (alle Angaben in MByte):

**Anzahl der Archivfile = Inhalt der Festplatte C: – hiberfil.sys – pagefile.sys / 2000**

Dies ist die etwaige Anzahl der vom DriveBackup produzierten Archivcontainer, wobei jeder die Größe von 2 GByte besitzt. Nachkommastellen werden noch oben gerundet. Zwei dieser Teilarchive gehen jeweils auf eine DVD. Haben wir gemäß dieser Überschlagsrechnung sieben Archive ermittelt, benötigen wir also vier DVD-RWs. **hiberfil.sys** und **pagefile.sys** können vom Gesamtinhalt abgezogen werden, denn DriveBackup nimmt statt ihrer nur zwei Platzhalter (Adressenangaben) mit ins Archiv und es werden während des Restore zwei neue Dateien dieser Größe auf der Festplatte am gleichen Platz erstellt. Nach dem ersten Start füllt Windows diese wieder mit allen aktuellen Daten.

## Start-CD brennen

Dies sollte die einfachste Übung sein und wir benötigen dazu einen ganz normalen CD-Rohling. CD-RW nehmen wir nur im äußersten Notfall. Sie sind auf Grund ihrer Qualitätsmerkmale wie ich schon erwähnte, kaum für eine längere Sicherung der Daten geeignet. Sie verlieren nach einiger Zeit ihre Daten.



Wir starten DriveBackup und klicken auf den Button **[Build Recovery Media]**. Nach einigen Sekunden öffnet der Assistent und bietet nach dem Klick auf **[Next]** uns zwei Möglichkeiten. Wir wählen die Einfachste und Sicherste (\*) **CD/DVD**. Nachdem wir wieder auf **[Next]** geklickt haben, ist die Eigenschaft gefragt und wählen (\*) **Typical**. Auf der nächsten Seite des Assistenten entscheiden wir uns für den Brenner und werden nun gefragt, wie schnell gebrannt werden soll. Da manche preiswerte Rohlinge oder Brenner bei maximaler Brenngeschwindigkeit überfordert sind, nehmen wir eine Geschwindigkeitsstufe niedriger. Noch ein Klick auf **[Next]** und unsere Start-CD wird gebrannt.

Diese CD ist praktisch der Schlüssel zur Lebensversicherung eures Systems und wird später nur noch benötigt, wenn Windows überhaupt nicht mehr starten will und der Verdacht besteht, das die Dateistruktur völlig zerstört ist. Diese CD wird mit einem wasserfesten Filzstift beschriftet und nachdem wir diese Anleitung abgearbeitet haben, sorgfältig aufbewahrt.

In diesem Zusammenhang möchte ich erwähnen, das bei Benutzung von (\*) **Advanced** die Möglichkeit besteht, zusätzlich noch ein Image, z.B. das was unmittelbar nach einer Erstinstallation von Windows erstellt wurde, ebenfalls auf eine Start-DVD zu brennen.

## Kurztest der Rettungs-CD

Um später nicht fassungslos festzustellen, dass die StartCD falls sie gerade mal gebraucht wird, nicht funktioniert, werden wir sie auch gleich einer Funktionsprüfung unterziehen. Wir legen die CD in Laufwerk und starten das System neu mit

### [Start] – Computer ausschalten - Neu starten.

Nach einer kurzen Bootsequenz befinden wir uns in einem Programmteil, welches Ähnlichkeit mit dem Bootmanager von Windows besitzt. In der Regel starten wir im **Normal Mode**. Damit wird ein MiniLinux als Betriebssystem geladen. **Save Mode** ist ein PTS-DOS und **Low-Graphics Save Mode** ein PDS-DOS in nur 16 Farben. Mit den unteren drei Menüpunkten wird von anderen Medien gestartet. Probiert die Menüs durch und informiert euch über ihre Möglichkeiten.



Sollte, aus welchem Grund auch immer, der PC nicht von der CD starten, müssen wir im BIOS-Menü die Einstellung der Bootreihenfolge ändern. Dazu führen wir einen Neustart des Systems aus und beobachten die Ausgabe des ersten Bildschirms, in welchem die einzelnen Laufwerke aufgezählt werden. An irgend einer Stelle steht geschrieben, welche Taste oder Tastenkombination gedrückt werden muss, um anschließend ins Menü des BIOS zu gelangen. Meist sind es **[Del]**, **[Entf]** oder **[F2]**, aber auch andere (Sonder)Tasten sind möglich.

Im Menü des BIOS suchen wir uns die Optionen, in welchen die Reihenfolge der Startlaufwerke festlegt. Mit Pfeil-, Bild- und Enter-Tasten (auch hier gibt es Abweichungen und Maus funktioniert nicht!) können die Seiten aufgerufen und die Abfragefolgen geändert werden. Dabei sollte an erster Stelle immer das CD/DVD-Laufwerk stehen. An zweiter Stelle die Festplatte und erst dann ein anderes Laufwerk, z.B. Diskette oder USB-Stick. Damit haben wir abgesichert, dass falls eine startfähige CD/DVD eingelegt ist, diese auch immer und in jeden Fall als Startmedium erkannt wird. Diese veränderte Reihenfolge birgt keinerlei etwaige Probleme beim Start und Betrieb.

Alle Menüpunkte des Bootmanagers sehen wir uns genauere an. Wichtig ist vor allem ist, dass in Notsituationen der Anwender nicht erst lange Fragen zu den Einstellungen stellen muss und er im Voraus schon weiß, welche Handlungen notwendig sind.

Selbstverständlich könnt ihr auch die einzelnen Modi ausprobieren.

## Menüführung im DriveBackup

Nun starten wir das erste mal DriveBackup unter Windows und machen uns mit seiner Menüführung vertraut. Diese unterscheidet sich wesentlich von der einer Vollversion und ist so organisiert, das sie den Anforderungen eines Erstbenutzers im vollem Umfang gerecht. Jede Aktion wird von Programm-Assistenten begleitet und dürfte auch für den Anwender verständlich sein, der einer englischen Sprache unkundig ist und nur ein paar Begriffe deuten kann.

Es wird mittels Klick auf einen Button die jeweilige Aktion eingeleitet. Bedeutungsvoll sind für uns die Button 2-5. Den Aktion des Button **[Build Recovery Media]** haben wir schon kennen gelernt. Der Button mit der Aufschrift **[Back up Disk or Partition]** ruft den Assistenten auf, welcher uns ein Image der Festplatte oder nur der Partition erstellen lässt. Große Bedeutung hat für unser erstes Imagearchiv der Button **[Check Archive Validity]**. Dieser Assistent prüft die auf DVD-RW gebrannten Archive auf ihre Qualität. Der Assistent, welcher mit dem Button **[Restore Disk or Partition]** aufgerufen wird, führt uns durch die Aktion der Wiederherstellung von defekter Festplatte oder Partition. Die Eigenschaft „defekt“ kann vieles bedeuten. Auch ein Infekt durch Malware.

Die an deren Button dürft ihr natürlich aus ausprobieren. **[Quick Start und User Guide]** ist eine sehr spartanisch gehaltene Hilfedatei in englischer Sprache. Mit **[Upgrade Now]** könnt ihr beim Hersteller eine Vollversion kaufen. Das ist aber kaum von Wichtigkeit, denn die Zeitschriften verteilen kostenlose DriveBackup und Festplattenmanager in bestimmten Zeitabständen. Ich habe es mal überschlagen, es müssen allein von diesem Hersteller 3,5 Mio Exemplare im Umlauf sein. Da aber kaum eine ernsthafte Reaktion der Zeitschriftenleser zu verspüren ist, gehe ich davon aus, das sie in der Restmülltonne gelandet sind. Noch heute können im <http://www.wekashop.de/> DVDs und bei Pearl.de Zeitschriften mit DVDs zum Spottpreis erworben werden, welche eines dieser Vollversionen beinhalten. Sie sind lediglich für professionelle Anwendung eingeschränkt jedoch für den Heimanwender voll nutzbar.

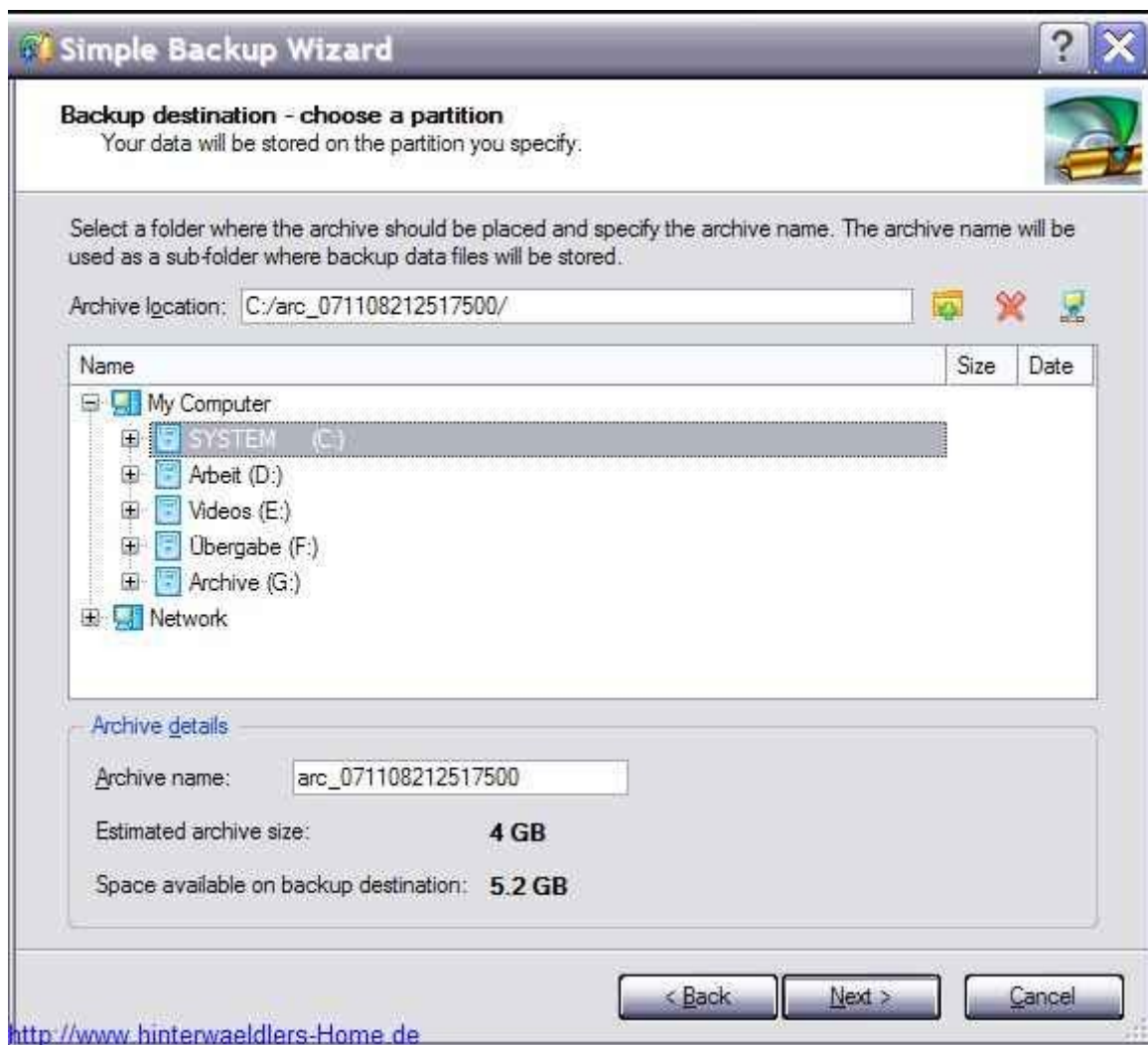
Die Button **[About]** und **[Exit]** bedürfen keiner Erklärung.

## Backup auf DVD erstellen

Dieser Vorgang wurde in den letzten Versionen stark vereinfacht. In DriveBackup Express sind es nur noch ein paar Mausklicks. Mit dem Klick auf den Button **[Back up Disk or Partition]** starten wir den Assistenten, der zunächst einen eigenen Dateisystemtreiber initialisiert und müssen ein paar Sekunden warten. Erhalten wir die Fertigmeldung gehen wir auf die nächste Seite. Dort wählen wir die zu sichernde Partition. Dies ist in der Regel das Windowslaufwerk C:.

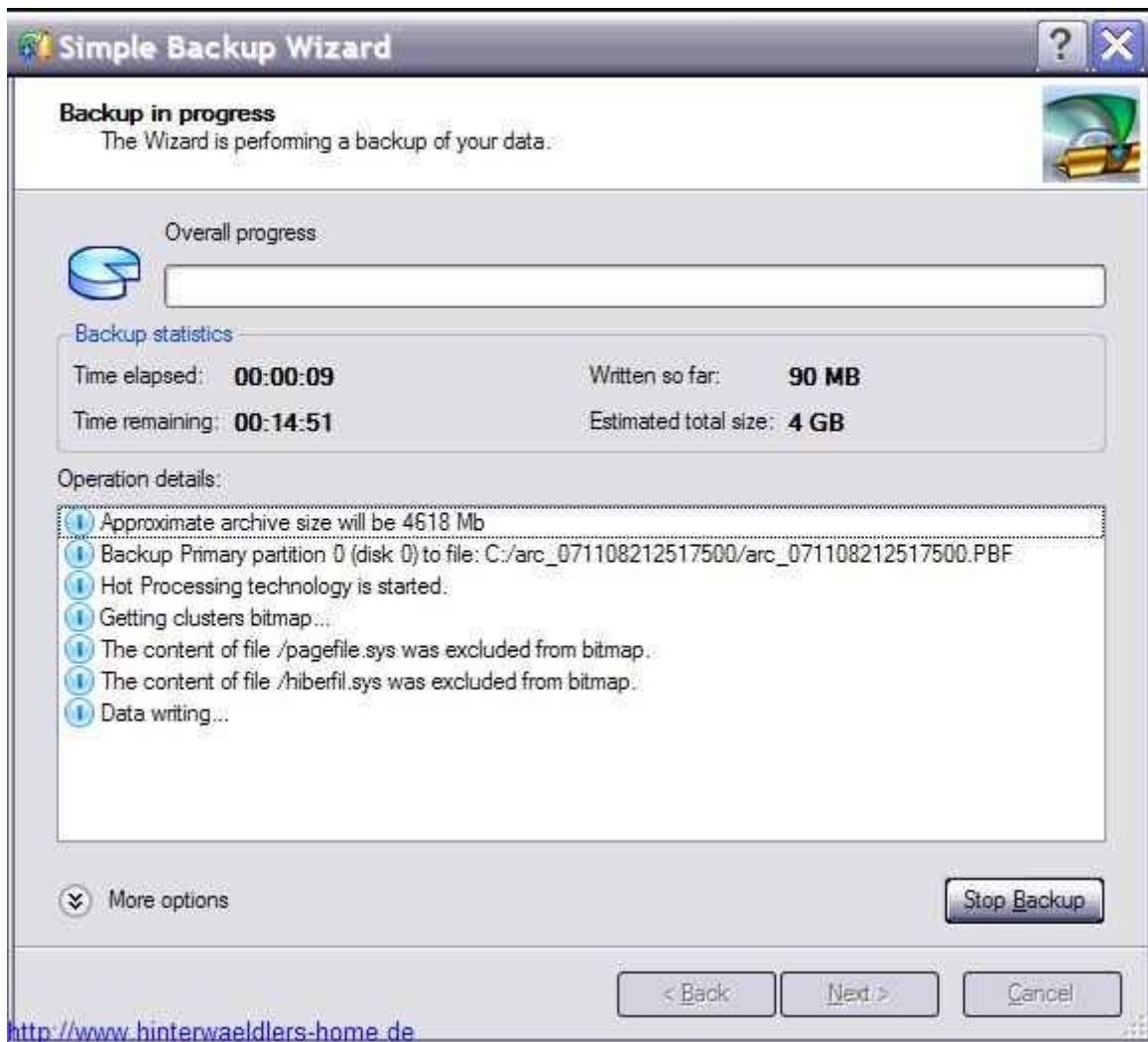


Zylinder 1 der HDD mit dem Master Boot Record lassen wir erstmal weg. Im gelben Messagefeld erkennen wir die Größe der gewählten Partition und wie groß das Archiv vermutlich wird. Eine Seite weiter werden wir gefragt, wo wir das Archiv speichern wollen und wie viel Platz auf der gewählten Partition ist. Im Regelfall ist dies auch die C:. Sollten noch andere Partitionen zur Verfügung stehen, können wir natürlich auch dort speichern.



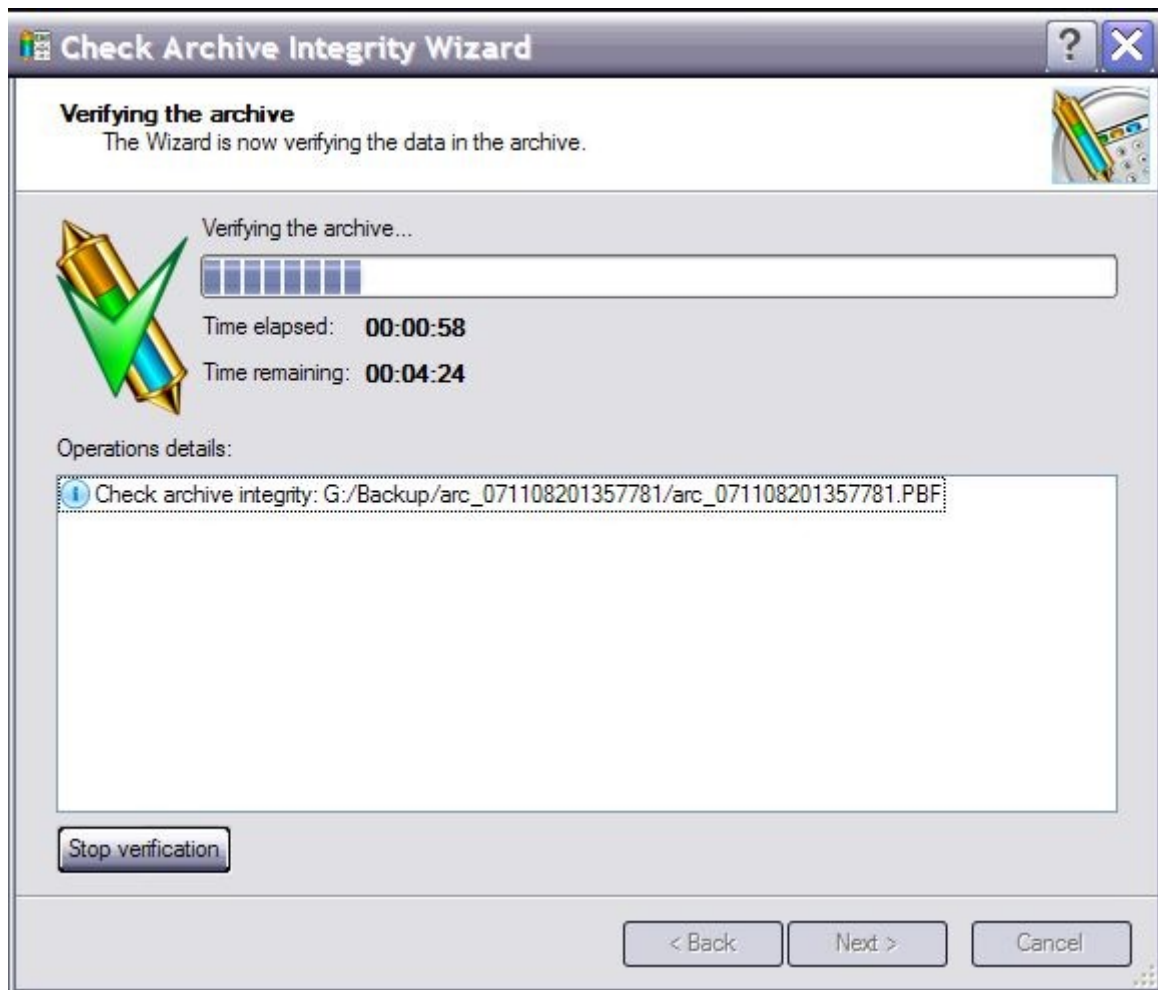
Im gezeigten Fall lesen wir, dass auf Laufwerk C: 5,2 GByte Platz ist und unser Archiv von 4 GByte problemlos erstellt werden kann. In diesem Zusammenhang können wir, falls Bedarf besteht, auch Verzeichnisnamen und den Namen des Archives ändern, welche vom Programm automatisch aus Datum und Uhrzeit zusammengesetzt sind. Haben wir die Aktion bestätigt, beginnt auch schon die Sicherung der Windows-Startpartition.

Wir lesen, dass zwei große Systemdateien nicht mit ins Archiv genommen werden. Nach wenigen Minuten ist unser Archiv fertig und wir finden es in einem neu erstellten Verzeichnis mit einem markanten Namen. Alle Teilarchive haben die Größe von 2 GByte. Nur die letzte Datei und die Beschreibungsdatei mit der Erweiterung .pfm ist logischerweise kleiner.



## Qualitätsprüfung des Backup

Mit einem Brennprogramm eurer Wahl brennt ihr nun die Dateien auf die bereitgelegten DVD-RW. Jede DVD-Hülle bekommt auch einen Zettel mit der Reihenfolge. Auf die erste DVD gehört auch die Beschreibungsdatei. Dieser Disktyp gehört auf Grund seines anderen physikalischen Aufbaus zu den sichersten optischen Datenträger. Trotzdem sollten wir das Ergebnis prüfen. Dies tun wir, nach einem erneuten Start von DriveBackup und einem Klick auf **[Check Archive Validity]**.



Dazu wir die erste DVD eingelegt. Im Dateiauswahldialog suchen wir das DVD-Laufwerk und wenn wir alles richtig gemacht haben, müsste die erste Datei ausgewählt werden können. Nach **[Next]** wird das Archiv auf eventuelle Defekte geprüft. Besteht unser Archiv aus mehreren DVDs meldet sich DriveBackup und wir werden aufgefordert, die nächste Disk einzulegen. Dies wird so oft wiederholt bis der Inhalt aller DVDs mit der Beschreibungsdatei verglichen sind. Sollte sich ein Defekt eingeschlichen haben, erhalten wir eine Meldung und brennen die bemäkelte Disk nochmal neu. Erst wenn alles fehlerfrei ist, gehen wir sicher, das unser Vorhaben gelingt.

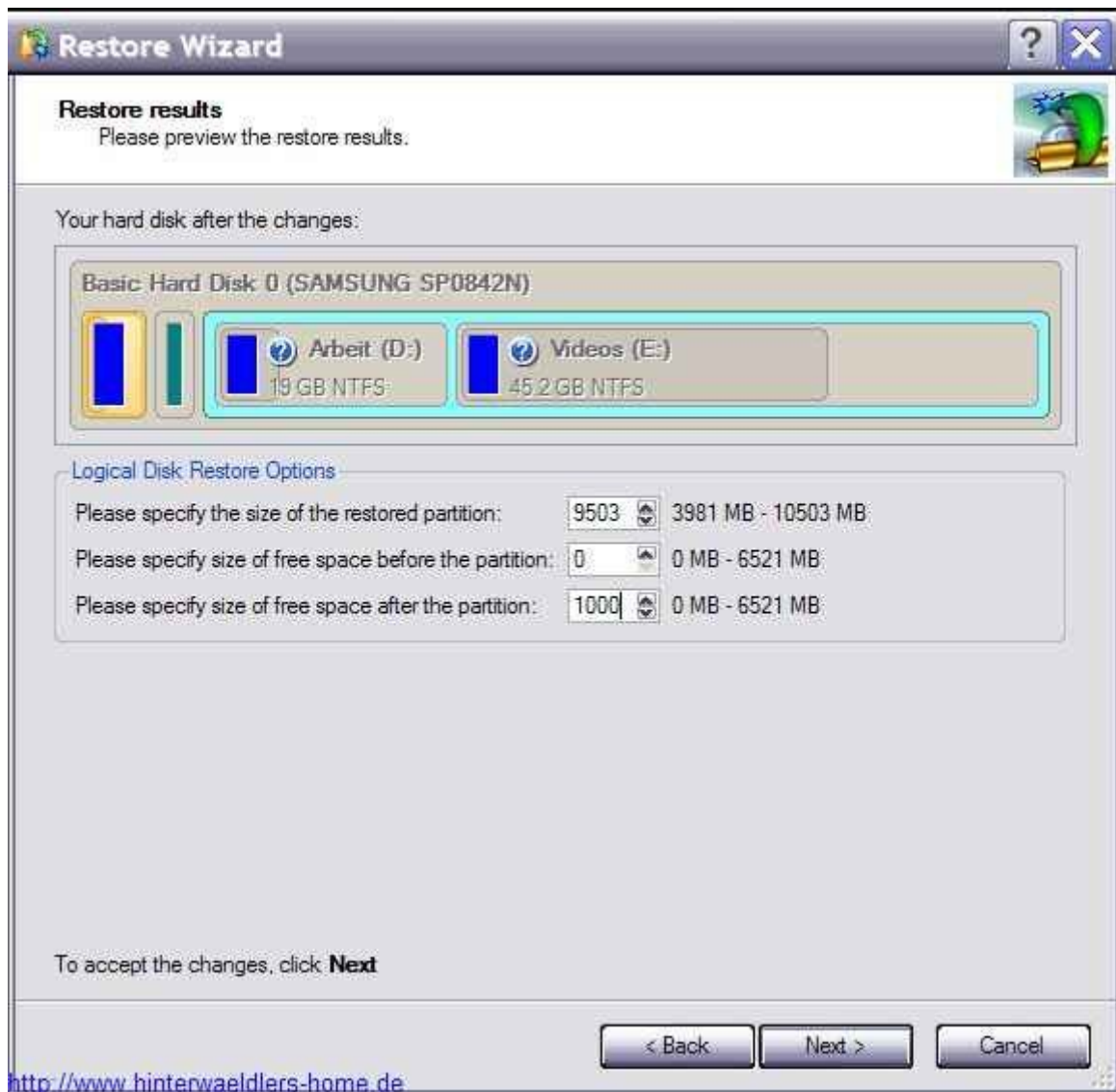
## Restore auf verkleinerter Partition C:

Ist nun endlich unseren Satz komplett und fehlerfrei, können wir auch gleich mit dem ersten Restore beginnen. Wir erstellen dazu eine neue kleinere Partition. Nach dem Start von DriveBackup legen wir die erste Backup CD ins Laufwerk und klicken auf **[Restore Disk or Partition]**.



Im Auswahldialog legen wir als Backupmedium das DVD-Laufwerk fest. Eventuell auf der C: noch befindliche Archive können nicht benutzt werden, da diese nach automatischer Löschung der Partition durch DriveBackup nicht mehr existent sind. Die nächste Frage von DriveBackup ist, welche Partition ersetzt werden soll. Selbstverständlich die C:

Nach dem obligatorischen **[Next]** und einer Sicherheitsabfrage wird diese Frage gestellt: (zu bemerken ist, dass dies auf meinen schon längst partitionierten HDDs gemacht wird und es sich logischer nur um eine Demonstration und nicht um die Realität handelt):



An dieser Stelle wird es möglich die Größe der C: neu festzulegen. Diese kann nicht größer als der frei Platz aber auch nicht kleiner als minimale Größe des Dateninhaltes der C: sein. Im Beispiel beträgt diese Größe 3981 MByte. Damit wir erstmal mit dieser neuen C: arbeitsfähig sein können, sollten wir nochmal 1 GByte zulegen. Im angezeigten Fall wäre die minimale Größe mit rund 5 GByte vorzusehen. Zur Demonstration habe ich am Ende der C: jedoch 1 GByte gekürzt. Diese Kürzung können wir in der Grafik auch optisch sehen.

Man kann aber auch anders vorgehen. Ihr packt in der grafischen Darstellung mit der Maus das rechte Ende der C: und zieht es soweit nach links, wie es möglich ist. Um nun die notwendige Arbeitsfreiheit auf der C: sicherzustellen, zieht ihr wieder 1-2 GByte nach rechts zurück und fertig. Theoretisch könnte man auch die Partition auf dem freien noch verschieben, das hat aber in unserem Fall keinen Sinn, sondern nur dann, wenn am frei werdenden Anfang ein neues Betriebssystem eingerichtet werden soll. Dies könnte Linux sein. Ein zweites Windows war noch nie eine gute Idee. Sorry, ich kenne keinen, bei dem sich ein derartiger Versuchsaufbau in Wirklichkeit und auf Dauer bewährte. Es war und ist auch in ferner Zukunft nur eine Spielerei ohne praktischem Nutzen.

Nachdem der C: die neue Größe zugeordnet wurde, ein Klick auf **[Next]** und es beginnt eine Aktion, die wie folgt beschrieben wird:

1. Oh Schreck, uns wird noch offensichtlicher Prüfung mitgeteilt, das dies nicht möglich ist, ob wir den Vorgang abbrechen oder den PC neu starten wollen. Häähhh? Haben wir etwa eine Demoversion? Natürlich nicht. Logischer Weise muss das System neu gestartet werden. Anders geht es nicht.
2. Der PC startet neu und statt Windows meldet sich die Konsole des Paragon.
3. Nach einigen Sekunden wird die aktuelle Partition C: gelöscht, neu formatiert und aus dem Inhalt der DVDs eine neue C: der gewünschten Größe auf die Festplatte geschrieben.
4. Besteht das Archiv aus mehreren DVDs wird nach dem Schreiben des Inhaltes zum Einlegen der Nächsten aufgefordert. Dies setzt sich bis zur letzten DVD fort.
5. Ist das Schreiben der C: beendet, startet der PC neu und (nochmal „Oh Schreck“) will Windows mit CHKDSK das System auf Fehler überprüfen, denn dessen Dateitabellen stimmen nicht mehr mit der Wirklichkeit überein. Wir sollten Windows gewähren lassen, denn einen Fehler wird es nicht finden.
6. Danach startet Windows noch einmal und unser Bildschirm erstrahlt in alten Glanz. In einigen wenigen Fällen kann Windows den Einstiegspunkt nicht finden und scheint in einer Endlosschleife stecken zu bleiben. Dies ist kein Fehler von Paragon. In diesem Fall hilft uns während einer erneuten Startsequenz die Sondertaste F8 und im erscheinenden Windows-Bootmanager wählen wir die letzte funktionierende Version.

## Ein wenig "trockene Theorie"

Jetzt, da Windows wieder unbeschädigt und tadellos auf einer wesentlich kleineren Partition funktioniert, werden wir unserer Festplatte zwei neue Partitionen spendieren und diese dem System zuordnen. Mit dieser Aktion wird es möglich, ein späteres Laufwerk D: als Arbeitslaufwerk und das dritte Lw E: als zukünftigen Lagerort für Archive jeglicher Art, auch für Drive Backup - Images benutzen.

Bevor wir das tun, erst einmal ein paar grundlegende Erläuterungen zum Aufbau der Festplatte und wie sie funktioniert. Wie wir schon während der Defragmentierung feststellen, versucht Defrag immer die Dateien an den äußeren Rand der Festplatte (in der graphischen Darstellung links) anzuordnen. Was ihm auch mehr oder weniger gut gelingt, denn am äußeren Rand der Scheiben befindet sich der schnellste Teil der Festplatte. Die inneren Teile sind die langsamsten und darum vermeidet das Betriebssystem diesen Bereich zu belegen. Damit wird dieser innere, langsamere Teil kaum benutzt.

Bei einer Aufteilung der Festplatte, so wie wir es bisher hatten, vermischen sich die Programmdateien mit den Daten permanent. So konnte es schon mal vorkommen, das riesige Movies aus dutzenden fragmentierten Teilen bestanden und sich Installationsarchive und Gigaspiele sich zwischen System- und Programmdateien drängten. Damit wurden **alle Dateien** immer mehr zerstückelt und das war eine der Hauptursachen, die unseren Festplatte fragmentierte und immer langsamer machte.

Zukünftig werden wir System&Programme von ihren Daten und den riesigen Spielen fein säuberlich trennen. Eine weitere Sortierung wird dann mit einer dritten Partition für die Archive und eventuelle Installations- und Setupdateien geschaffen. Diese Aufteilung hat zudem noch den Vorteil, dass falls die Festplatte C: mit dem Betriebssystem mal crasht oder von Schadsoftware befallen ist, die anderen Partitionen davon kaum betroffen sind. Die Daten bleiben erhalten. Da sie kaum ausführbare Dateien enthalten und damit viel weniger gefährdet sind, gehen sie nicht mehr verloren, so wie früher im Verzeichnis *C:\Dokumente und Einstellungen\... usw.* Dies ist bekanntermaßen auch der Hemmschuh bezüglich der Löschung der C: und das Ergebnis ist, das im Internet von sehr ernstzunehmenden Fachleuten behauptet wird, das Deutschland nicht nur Weltmeister im Biertrinken sondern auch im Malwarebesitz ist. Eine Schwachstelle im Zusammenhang mit Mozilla&Co werden wir später auch noch beseitigen.

Die innerste Partition als "Lagerplatz" für die Dateien, die kaum in maximaler Geschwindigkeit zur Verfügung stehen müssen, bietet sich direkt an und dieser Platz wird einer aktiven Nutzung zugeführt. Je besser uns diese Trennung von Programmen, Daten und Archiven gelingt, desto schneller wird Windows im täglichen Betrieb arbeiten und um so sicherer ist das System.

Wenn wir regelmäßig die ganze Partition C: von unbrauchbaren Müll beräumen, einem Backup unterziehen und das Image auf der innersten Partition lagern, können wir bei Bedarf Ruck-Zuck innerhalb nur weniger Minuten den von uns "eingefrorenen" Zustand wieder herstellen. Damit hat der PC eine kaum noch zu übertreffende Sicherheit erreicht. Zwar sollten wir so wie bisher den Virenschoner und die anderen Sicherheit bietenden Programme aktuell updaten, aber ein Virenbefall, ein Einnistern von Würmern, Trojanern und Dealer etc. hat für uns jeden Schrecken verloren. In diesem Fall wird dem Scanner keine Schutzfunktion mehr übertragen, sondern er ist einer von mehreren Indikatoren dafür, ob unser System schon kompromittiert ist oder nicht.

Eine etwaige Unkerei von Fachautoren der Bunten oder selbst ernannten Fachleuten verweisen wir großzügig ins Bereich der Märchen und Legenden. In der Praxis überdauert die Standfestigkeit einer Festplatte die Lebensdauer eines PC/Schlepptop, es sei denn er befindet sich ständig im Kofferraum eines PKW oder wird zum Fußball deklassiert und eine Malware welche Images infiziert und unbrauchbar macht, wie der Testbericht in einer Ausgabe des PCM kürzlich vermuten lies, hat es unter den bisherigen mehreren 100.000 Viren noch nicht gegeben.

Einen weiteren Vorteil besitzt unsere neue Anordnung:

Immer wieder werden wir mit neuen und manchmal angeblich besseren Programmen aus Zeitschriften und dem Internet überschüttet. Oft können wir den Verlockungen nicht widerstehen und installieren diese. Während des Probetriebes stellt sich allerdings heraus, das sie ausgesprochener unseriöser Schiet sind. Jetzt wollen wir deinstallieren und wie das bei solchen Programmen so üblich ist, unmöglich. Bisher blieb uns nur das Löschen der Verzeichnisse übrig. Ihr kennt das. Keiner wusste, wohin deren Setup noch Dateien und vor allem welche, installiert hat und wohin Einträge in die Registry geschrieben wurden. Jetzt nur 6 Minuten Restore und fertig. Ehrlich, das ist so. Die Zeit reicht nicht mal aus, um eine Tasse Kaffee zu brühen und sie zu trinken. Danach könnt Ihr euch sofort über Internet beim Programmierer beschweren. Nicht bei der Zeitung, dieser schickt ihr höchstens einen netten Hinweis.

In diesem Zusammenhang sollte auch noch die zu erwartende Geschwindigkeit besprochen werden:

- Bei der Arbeit mit DVDs ist deren maximal mögliche Schreib- und Lesegeschwindigkeit hauptverantwortlich. Dies ist eine physikalische Grenze, an der wir nichts drehen können. Ein Ausweg wären mobile Festplatten, diese fallen aber nicht in das gewünschte Preissegment. Dazu kommt noch, falls die Startpartition restlos zerstört ist und sich darum DriveBackup auch nicht mehr starten lässt, wir von der Rettungsdisk installieren müssen und deren BS noch weniger Speicherbereich für diese Aktion bietet. Andererseits ist das Image auf DVD-RW oder gar DVD-RAM der sicherste und zuverlässigste Aufbewahrungsort.
- Da zukünftig das Backup auf die Festplatte geschrieben und das manchmal notwendige Restore mit der Paragon-Konsole von da gelesen wird, kann man je nach Prozessor- und Festplattentyp von einer Geschwindigkeit für Backup und Restore von 8 - 15 MByte/Sek ausgehen. Das ist eine schon sehr beachtliche Leistung.

## Weitere Partitionen erstellen

Um der Festplatte weiteren Partitionen hinzuzufügen, benutzen wir den Festplattenmanager von Windows. Diesen hat MS sehr gut versteckt. Zum Aufruf gehen wir über [Start]-Ausführen.... In die Editorzeile geben wir **C:\WINDOWS\system32\diskmgmt.msc** ein und drücken die **[Enter]**-Taste. Wir befinden uns in der Datenträgerverwaltung. In seiner graphischen Darstellung erkennt ihr, den nun frei gewordenen Platz nach der Partition C: Dort richtet ihr noch zwei weitere Partitionen ein. Mit dem Programm-Menü gelingt das ohne Problem.

Zuerst die eben besprochene Partition für Archive. Vom Manager wird gefragt, wo ihr sie anlegen wollt. Nach ein wenig probieren gelingt das. Die Größe dieser Partition legen wir mit ca. 20 GByte fest. Sie ist abhängig von der Gesamtgröße der Festplatte und kann abweichen. Bei mir sind es lediglich 10 GByte. Mehr Platz wird für diese Zwecke kaum benötigt. Im FreeCommander bzw. Explorer finden wir es Laufwerk mit dem Bezeichner D: und verschieben zuerst alle im Laufe der Jahre sich angesammelten Setup- und Install-Dateien. Alles wird ordentlich in eindeutig benannten Verzeichnissen verstaut. Auf der C: verbleiben nur das Betriebssystem sowie die von uns ständig benötigten Programme und deren Konfiguration.

Unsere System ist wieder schlanker geworden und erstellen nochmal ein Backup. Diesmal jedoch legen wir als Zielspeicherort das neue Laufwerk fest. Damit habt ihr euer erstes Image auf der Festplatte. Ihr startet wiederum DriveBackup und macht nochmals ein Restore auf eine verkleinerte Partition C:. Dies geht jetzt gegenüber dem Lesen von DVDs unvergleichlich schneller. Die endgültige Größe ist abhängig von den benutzten Programmen. Bei meinem XP beträgt sie 11 GByte. Beim aktuellen Vista und dem größeren RAM sind 20 GByte denkbar. Mehr jedoch kaum, übertreibt es nicht.

Zuletzt wird der verbliebene Platz partitioniert. Ob es eine oder zwei Partitionen sind und eine von Beiden verschlüsselt wird, könnt ihr selbst entscheiden. Überdenkt auch die Situation mit eventuellen Spielen. Mehr Platz als für drei Spiele wird kaum benötigt. Irgend wann habt ihr eines davon bis zum Erbrechen gespielt und es noch auf CD bzw. DVD oder etwa nicht? Dann wird es Zeit. Rohlinge kosten nicht die Welt.

Einige von euch kauften ihren PC beim Lebensmitteldiscounter und besitzen statt einer Setup CD eine Recoverypartition inkl. einer RecoveryCD. Auch bei Laptops unterschiedlicher Hersteller ist diese Praxis üblich. Diese Partition darf nicht angetastet werden, solange ihr keine Windows Setup CD besitzt. Also Finger davon und nicht einfach mit einem Partitionsmanager löschen. Bequemlichkeit hat ihren Preis! Wie ihr später trotzdem noch zu einer Setup CD kommt, müsst ihr einfach mal im Internet erfragen. Es ist auch möglich, das Recoverysystem zu installieren, darauf alle blödsinnigen Programme (welche noch nie echt benutzt wurden) deinstallieren, das ganze dann mit Servicepack und Updates aktualisieren sowie mit DriveBackup sichern. Nun, wenn ihr später den Inhalt dieses Recoverylaufwerkes auf einer DVD oder auf CDs habt, kann auch dieses Laufwerk von mehreren GByte Größe von euch gelöscht und einer sinnvolleren Verwendung zugeführt werden. Es lässt sich ja jederzeit wieder rekonstruieren.

## *Festplatte endgültig einrichten*

Hier bleibt nicht mehr viel zu tun. Über das meist habe ich Euch schon unterrichtet. Auf das zuletzt erstellte Laufwerk verschiebt ihr die Dateien am besten mit einem Dateimanager in 2-Fenster-Technik, ähnlich dem NortonCommander. Neben dem von mir vorgeschlagenen **FreeCommander** ist auch der **A43** von <http://www.snapfiles.com/get/a43file.html> hervorragend geeignet. Dieser lässt mehrere auf dem Desktop frei bewegliche Fenster, einschließlich Verzeichnisbaum und diversen Extras zu.

Dateien, welche Ihr nicht mehr auf der C: benötigt, erhalten auf dem neuen Laufwerk D: einen dauerhaften Platz. Spiele von der Größe einiger CDs und Movies von vielem GByte Größe sowie die Musik- und Bildersammlung können sich hier tummeln. Auch Arbeitsverzeichnisse großer Anwendungen befinden sich hier und letztlich sind eure persönlichen Dokumente in einem Verzeichnis D:\Arbeit\Briefe\Beschwerden an BG\\*. \* sicherer aufgehoben als im vom Herrn MS festgelegten Verzeichnis auf der C:. Alle seriösen Anwendungen können so eingerichtet werden, das sie ihre Dateien dort ablegen, wo Ihr es bestimmt. Auch die Download-Manager kann man dazu dauerhaft überreden. Ihr werdet sicher noch viele Anwendungsmöglichkeiten für dieses Laufwerk finden. Letztlich gibt es Programme, die von CD/DVDs virtuelle Laufwerke einrichten können. Auch diese Laufwerke haben dort einen guten Platz.

# Profil des Firefox verschieben

Ich versprach euch noch etwas für Moz.&Co zu tun. Das Problem ist, das beim Restore der C: nicht nur die Malware oder defekte Systemdateien verschwinden, sondern eben auch eure Internet-einstellungen und Mails sind verdunstet. Iherwegen habe ich schon von vielen Tränen gelesen. Die Wiederherstellung derart verschwundener Mails und Adressen ist zwar grundsätzlich möglich, aber kaum bezahlbar. Darum wird nachfolgend eine Lösung angeboten, welche von mir schon viele Jahre praktiziert wird.

Auch hier bewährt sich ein Dateimanager mit Zweifenster-Technik. Er ist so einzustellen, das auch versteckte und Systemdateien angezeigt werden. Nur so kann fehlerfrei gearbeitet werden. Beim FreeCommander sind die Einstellungen unter **Menü - Extras - Einstellungen - Ansicht** vornehmen

1. ein leeres Profilverzeichnis auf einer anderen Partition mit Dateimanager anlegen.  
zB: D:\Mozilla-Profile\Firefox
2. in das Programmverzeichnis des Firefox gehen und den Profilmanager mit **Firefox -P** aufrufen
3. ein neues Profil mit Namenszusatz (zB. Standard-neu) im dafür bestimmten Verzeichnis auf anderem Laufwerk anlegen.
4. Firefox im Profilmanager öffnen und sofort wieder schließen.
5. mit dem Dateimanager kontrollieren ob das Profil tatsächlich existiert.
6. im ersten Fenster des Dateimanagers das ursprüngliche und im Zweiten das neue Profilverzeichnis öffnen
7. alle Dateien aus dem Alten in das neue Verzeichnis **kopieren** (alles überschreiben)
8. Profilmanager von Firefox wieder aufrufen und das ursprüngliche Profil löschen
9. Firefox starten und fertig.
10. bei mehreren Benutzern des PC ist diese Maßnahme für alle durchzuführen

Noch bestehende Reste der alten Profile (profiles.ini, pluginreg.dat etc.) verbleiben im ursprünglichen Verzeichnis. Darin stehen jetzt die Verweise auf den neuen Speicherort.

Das wird analog mit Thunderbird und jeder beliebigen Mozilla-Anwendung durchgeführt. Nach dieser Maßnahme kann jederzeit die Startpartition mittels Image neu geschrieben werden, ohne das es zu einem Daten-, Mail- oder Adressenverlust kommen kann.

## Neues Backup auf Festplatte erstellen

Habt Ihr eure Verzeichnisse auf der D:\ eingerichtet und die Daten und Profile von Mozilla&Co dorthin verschoben, ist das Laufwerk C: um vieles schlanker und effektiver. Um der neuen Datenorganisation das i-Püñktchen aufzusetzen, wird gleich noch mal Müll entsorgt und defragmentiert, ähnlich wie ihr es anfangs getan habt. Ihr merkt schon, es geht um vieles schneller und es wird ab jetzt auch immer so sein.

Auch kann die Systemwiederherstellung abgeschaltet werden, denn sie war bisher ein beliebter Ort dafür, das nachdem ein Trojaner eine Malware nachgeladen und installiert hat, er sich selbst einen Wiederherstellungspunkt setzte und danach von der nachgeladenen und konfigurierten Malware gelöscht. Wurde nun tatsächlich die Malware identifiziert und nach alten Geheimrezepten eine Systemwiederherstellung durchgeführt, begann und das Spielchen von neuem. Weiterhin können wir oft nicht sagen, was bei einer Systemwiederherstellung tatsächlich passiert und wundern uns, das Programme zwar noch vorhanden, jedoch funktionsunfähig sind.

Nun werden wir ein erneutes Backup machen. Diesmal jedoch nicht um wieder neue Laufwerke einzurichten, sondern insbesondere das jetzt bestehende Betriebssystem und eure aktuelle Programmzusammenstellung zu archivieren. Damit wird es möglich, jederzeit genau diese aktuelle Installation wieder herzustellen. Das war bisher weder mit einer Recovery-Installation von Windows und noch weniger mit der Systemwiederherstellung von Windows XP durchführbar.

Alle bisherigen Archive können gelöscht werden, denn sie waren gewissermaßen nur Zwischenstationen auf dem langen Marsch. Wir starten also wieder DriveBackup und klicken auf **[Back up Disk or Partition]**. Jetzt achten wir besonders darauf, das das richtige Ziellaufwerk und Zielverzeichnis angegeben ist. In diesem Fall wird später das Archiv vom Programm verwaltet. Auch einen Kommentar lohnt sich jetzt auszufüllen und schreiben zum Beispiel unverwechselbar, das es das erste ordentliche Backup ist.

Nach wenigen Minuten ist DriveBackup fertig und die Archivcontainer von jeweils 2 GByte Größe sowie die Beschreibungsdatei werden auf eine DVD-RW oder besser auf DVD-RAM gebrannt.

Für ein späteres Backup (mal ganz schnell zwischen durch), ist eine Kopie auf DVD kaum notwendig. Eine Sicherung anderer Partitionen ergibt für den ONU auch kaum einen wirklichen Sinn. Die angelegten Arbeitsverzeichnisse auf der D:\ sind in ständiger Ergänzung und Erweiterung. Sie können bei Bedarf regelmäßig mit einem herkömmlichen Backup oder einem Packprogramm auf Diskette, USB-Lw oder ein anderes Medium gesichert werden. ZipGenius von <http://www.zipgenius.it/> und KW's DatenBackup von <http://software-by-kw.de/wb/pages/home.php> sind bestens geeignet. Auch andere Lösungen sind bei Bedarf denkbar. Man muss also nicht immer die schweren Geschütze auffahren.

# Restore von Festplatte

Setzen wir unserm Bemühungen die Krone auf und erstellen das erste Mal ein Restore von der Festplatte und üben so den Ernstfall. Wir wählen wieder

## **[Restore Disk or Partition]**

Das nun schon bekannte Frage&Antwort-Spielchen beginnt erneut. Haben wir alle Fragen richtig beantwortet, wird wieder unser PC nach unten gefahren und die Konsole gestartet.

Das Restore erfolgt nun in einer nicht mehr zu überbietenden Geschwindigkeit. Als ich dies das erste Mal erlebte, glaubte ich ernsthaft an einen Fehler. Ganze 6 Minuten um eine von Malware infizierte Partition wieder herzustellen. Ich war fassungslos. Aber es ist Tatsache und vollendet.

In diesem Zusammenhang muss noch erwähnt werden: Paragon DriveBackup 9 Express ist umwerfend einfach aufgebaut und spartanisch zu bedienen. Einfacher geht es wirklich nicht. Das Tool hat aber auch vorsätzlich eingebaute Nachteile. Ein wesentlicher ist, dass es die Dateien nicht komprimiert im Container speichert. Sie werden also größer als ihr es von ähnlichen Tools gewohnt seid.

Wenn ihr also in den nächsten Monaten nicht mehr zufrieden seid und zu einer Vollversion wechseln wollt, dann könnt ihr es ohne Nachteile tun. Die Archive sind untereinander kompatibel. Die Vollversion kann jederzeit die Archive des Express entpacken, genau so wie die Konsole des Express mit den hoch komprimierten Archiven von DriveBackup oder dem Festplattenmanager umgehen kann. Höhere Kompression hat natürlich auch ihren Preis mit etwas geringeren Geschwindigkeiten.

Das gehört hier nicht her: Die höchste Geschwindigkeit in den beiden Modi Backup und Restore, bei einer Kompression die allen anderen überlegen ist, besitzt SelfImage in Verbindung mit einer BartPE Muuhhhaaa

# Pflege des Image

Auch ein Image bedarf wie jedes andere Programm einer Pflege. Wenn wir nicht darauf achten ist es innerhalb weniger Monate total veraltet und der Anwender steht vor eine schwer lösbaren Aufgabe.

Wir führen am Besten unmittelbar nach jedem zweiten Dienstag im Monat (Patchday) diese Tätigkeit durch. Wie ist nun die von mir vorgeschlagene Reihenfolge:

1. Zunächst überlegen wir uns, welche der im vergangenen Monat installierten Programme sich bewährt haben und wir behalten möchten. Dies gilt natürlich auch für eventuelle Programmupdates. Deren Setup behalten wir und alles andere wird gnadenlos entsorgt. Wir sind keine Müllsammler.
2. Deinstalliert oder entmüllt muss nichts werden, denn als erstes führen wir ein Restore des C:-Image durch. Damit ist abgesichert, das nicht nur Müll sondern auch unbemerkt eingeschlichene Malware das Zeitliche segnet.
3. Als nächstes bringen wir den PC mittels Script von <http://www.ntsvcfg.de> auf seine ursprüngliche Konfiguration (Option 4). Systemneustart.
4. Wir öffnen jetzt das wieder verfügbare Sicherheitszentrum und klicken auf die Zeile „Automatische Updates“ und dort auf die Zeile „Updates von MS Webseite installieren“ oder so. Der nun folgende Vorgang sollte bekannt sein.
5. Im Anschluss wird die notwendige Sicherheitskonfiguration mit dem Script von <http://www.ntsvcfg.de> wieder hergestellt. Neustart des Systems.
6. Nun installieren wir alle vorhandenen Programmupdates und updaten die Signaturdatenbank des Scanners.
7. Wir löschen das vorhandene Image und erstellen ein Neues.
8. Bei Bedarf kann das komplette Image auf DVD-RW bzw. DVD-RAM gebrannt werden. Kleinen Zettel dazulegen! Nicht beschriften.

Dieser Vorgang dauert bei mir nicht länger als 30 Minuten und ich bin überzeugt, das es bei euch ebenfalls kaum länger dauern wird. Kommt es zwischenzeitlich zu einem Desaster beträgt der zeitliche Aufwand zur Herstellung eines definierten System-Zustandes nur wenige Minuten. Man muss also gar nicht mehr überlegen und stunden- oder tagelang suchen, mit welchen Programm ein vermutlich erfolgreicher Angriff durch Malware abgewehrt werden könnte. Der Start von DriveBackup nach einem Verdacht reicht.

## *Ein kleines Nachwort*

Wenn man sich überlegt, wie lange allein Windows XP benötigt, um sein Betriebssystem zu installieren. Dann wird offensichtlich, welcher Fortschritt mit diesem Werkzeug auf unseren PC gekommen ist. Dazu kommt, das unser Computer nicht nur sein Betriebssystem wieder hat. Nein, wir haben auch alle Anwendungen im sofort gebrauchsfähigen Zustand. Ihr könnt unmittelbar danach auf die Daten anderer Partitionen zugreifen. Selbst das Internet funktioniert wieder, als wäre nichts geschehen. Wir brauchen weder Windows XP noch irgend eine andere Anwendung beim Hersteller anmelden oder neu registrieren. 6-10 Minuten je nach Geschwindigkeit des PC und Datenmenge, fertig!

Wie viele Tage wurde Letztens von euch benötigt, um nach einem Supergau eine identische Festplatte wieder herzustellen und ... gelang dies überhaupt? Die Verwirklichung dieser Anleitung nimmt jede Horrorvision und zwanghafte Sicherheitslösung, die euer System zur Schnecke macht. Sicherheitssoftware ist wie Rauschgift. Hat man erst einmal an ihr geschnüffelt, will man immer mehr und immer härtere Sachen. Der Newcomer glaubt ohne sie nicht mehr auszukommen und euer System landet dann genau dort, wovor ihr es eigentlich schützen wolltet. Denkt mal drüber nach. Ich habe nicht umsonst versucht, jeden kleinen Schritt zu beschreiben und zu begründen. Für mich wäre es einfacher gewesen, 10 oder 12 Sätze zu schreiben und es euch überlassen, ob ihr wollt der nicht wollt.

Noch was wollte ich nicht unerwähnt lassen. Ich habe mich auf das kostenlose und für jeden im Internet erhältliche DriveBackup 9 Express bezogen. Eine ähnliche oder gar noch bessere Lösung ist mit den gleichfalls oft kostenlosen Personalversionen von Paragons DriveBackup, ExactImage und Festplattenmanager sowie Acronis TrueImage und in Verbindung mit einer BartPE oder einer WinBuilder – VistaCE - Lösung auch SelfImage, DriveSnapshot oder DriveImageXML möglich. Das meiste von dem was hier beschrieben wurde ist auf diese LiveCDs zweifelsfrei übertragbar.

Wer unbedingt das Teuerste beim Händler sich aufschwätzen lässt ist unrettbar unbelehrbar.

Ich wünsche euch viel Spaß mit einem Imagingprogramm.  
der hinterwäldler