Datensicherung und Datensicherheit

Dokument erstellt von:	Peter Sodermanns
begonnen am:	22. November 2006
gespeichert unter:	G:\Text\FotoClub\KN_Datensicherung_und_Datensicherheit.odt
letzte Änderung:	20. Februar 2007

Inhaltsverzeichnis

1 Einleitung

Wie kann man das wichtigste Gut des Digitalfotografen – die Bilddateien – vor Verlust durch Hardware-Defekte, Unachtsamkeit oder gar Diebstahl schützen?

Die Hauptursache für Datenverlust ist der Benutzer selber: Es passiert leicht, dass man sich beim Löschen von Dateien vertut und die falsche Datei oder das falsche Verzeichnis markiert. Oder man bearbeitet eine Bilddatei und überschreibt aus Versehen das wertvolle Original, statt den "Speichern unter"-Dialog zu verwenden.
Die zweithäufigste Ursache für Datenverlust ist ein mechanischer oder elektrischer Defekt der Festplatte. Während meiner über zwanzigjährigen PC-Nutzung ist mir das bereits dreimal passiert, und beim ersten Mal habe ich auch nicht wieder beschaffbare Daten verloren. Aus Schaden klug geworden, verfüge ich seitdem stets über Sicherungskopien der wichtigen Daten.
Die dritte Ursache ist der Verlust des Datenträgers selber, sei es durch eigene Unachtsamkeit oder durch Diebstahl. Auch um diesem Fall vorzubeugen, ist die Kopie der Daten unverzichtbar. Zusätzlich ist jedoch eine Verschlüsselung der Daten sinnvoll, damit der Finder bzw. Dieb nur in den Besitz einer Festplatte kommt, aber keinen Zugriff auf den wertvollen Inhalt erhält.
Schlussendlich sind Katastrophen zu berücksichtigen wie Brand oder Erdbeben. Menschen neigen dazu, solche Risiken gering zu bewerten, und sie glauben, sie persönlich seien davon schon nicht betroffen. Trotzdem haben die Meisten eine Hausratversicherung. Bei einem Wohnungsbrand kann jedoch keine Versicherung die zerstörten Daten wieder herstellen.

Dem Verlust der Daten kann man durch rechtzeitiges Kopieren (Thema **Datensicherung**) vorbeugen, Verschlüsselung schützt davor, dass Daten in falsche Hände geraten (Thema **Datensicherheit**).

Für beide Falle werden im Folgenden Strategien beschrieben, die – je nach Sicherheitsbedürfnis – mit unterschiedlichem Aufwand zu realisieren sind.

2 Daten – was ist das überhaupt?

Jede Information, die im Computer gespeichert ist, wird als "Daten" bezeichnet, und wird durch eine Folge von Einsen und Nullen bezeichnet, den Bits. Den Buchstaben "A" beispielsweise kennt der PC als "00100001", was der dezimalen Zahl 65 entspricht. Jedem Buchstaben ist eine solche 8-Bit lange Zahl zugeordnet, ebenso den übrigen, druckbaren Zeichen. Der so definierte "Zeichensatz" kann 2^8 = 256 Zeichen unterscheiden.

Zusammengehörige Daten, also zum Beispiel die Buchstaben dieses Textes oder die Informationen eines Bildes, werden in "Dateien" zusammengefasst.
Die Dateien werden im Computer auf der Festplatte gespeichert, einem Datenträger mit rotierenden Magnetscheiben, auf den die Datenbits (die Einsen und Nullen) in sequentieller Folge in Form von Magnetisierung winzigster Bereiche abgespeichert werden.

2.1 Das digitale Bild

Das digitale Bild ist eine Ansammlung von Bildpunkten, die über Farbwerte verfügen. Die Farbwerte sind Zahlen, die die Helligkeit des Rot-, des Blau- und des Grünanteils beschreiben.
Die Datei, in der das Bild gespeichert ist, besteht daher aus einer Folge von Zahlen, pro Bildpunkt drei Zahlenwerte. Der Farbumfang ist durch den Wertebereich dieser Zahlen vorgegeben. Üblich sind 8-Bit-Werte, also 256 Abstufungen pro Farbe, und 16-Bit-Werte, also 65.536 Abstufungen.
Mit 8-Bit-Werten können 16.777.216 verschiedene Farben dargestellt werden, mit 16-Bit-Werten ca. 281.474.976.700.000 (Billiarden) verschiedene Farben.
Ein Bild von 8 Megapixeln hat 8.388.608 Bildpunkte, also 25.165.824 Bytes bei 8-Bit-Darstellung und das Doppelte bei 16-Bit-Darstellung. Wenn ein solches Bild als TIFF-Datei gespeichert wird, bekommt man eine Datei von rund 50 GB Größe.

Eine Übersicht für verschiedene Kameraauflösungen in Megapixeln:

Bild in Megapixeln	Anzahl der Bildpunkte	Speicherplatz 8 Bit (unkomprimiert)	Speicherplatz 16 Bit (unkomprimiert)
6	6.291.456	18.874.368	37.748.736
8	8.388.608	25.165.824	50.331.648
10	10.485.760	31.457.280	62.914.560
12	12.582.912	37.748.736	75.497.472

2.2 Dateiformate

Wegen der immensen Datenmengen werden Bilddaten in komprimierter Form gespeichert. Unkomprimierte Dateiformate werden in Kameras nicht mehr verwendet. Bei den komprimierten Formaten muss man unterscheiden zwischen verlustfreier und verlustbehafteter Komprimierung.

Das JPEG-Format ist wegen seiner relativ geringen Dateigrößen sehr weit verbreitet, insbesondere im Internet, erkauft diesen Vorteil aber mit verlustbehafteter Kompression.
D.h. aus einer solchen Datei lässt sich nie mehr das Originalbild rekonstruieren. Der Kompressionsgrad ist beim Speichern einer JPEG-Datei einstellbar und wird als Qualität angegeben: 100% bedeutet optimale Bildqualität (und –größe), kleinere Prozentzahlen liefern stärkere Kompression und damit kleinere Dateien, aber auch stärkere "Klötzchenbildung". Je stärker ein JPEG-Bild komprimiert ist, desto hässlicher wird es beim Vergrößern.

Aber auch eine Qualitätsstufe von 100% liefert bereits ein komprimiertes Bild und ist damit weit von der Originalqualität und –auflösung entfernt.
JPEG-Dateien eignen sich nicht zur Bildbearbeitung, denn bei jedem Speichern der Datei wird erneut komprimiert, so dass die Qualität nach jedem Bearbeitungsschritt weiter abnimmt.

Eine gebräuchliche Form der verlustfreien Komprimierung ist das TIFF-Format, das von allen Bildbearbeitungsprogrammen unterstützt wird und früher in Digitalkameras verwendet wurde, um die Bilder in höchster Qualität zu speichern. TIFF-Dateien sind rund 5x größer als das JPEG-Pendant in maximaler Qualität, sind dafür aber sehr gut für die Bildbearbeitung geeignet, da sie beliebig oft ohne Qualitätseinbußen gespeichert werden können.

Die für den ambitionierten Digitalfotografen wichtigste Speicherform ist das RAW-Format, ein herstellerspezifisches Dateiformat mit verlustfreier Komprimierung und ggf. Zusatzinformationen. Als Ausgangspunkt für die Bildbearbeitung ist dies die erste Wahl, sofern die Kamera dieses Format anbietet.
Ein Nachteil des RAW-Formats ist, dass es nicht genormt ist, jeder Hersteller hat hier seine eigene Definition, die oft auch von Kameramodell zu Kameramodell unterschiedlich ist. Beispielsweise benutzt die Canon EOS 400d ein anderes RAW-Format als das Vorgängermodell 350d. Hier sind die Hersteller von Bildbearbeitungsprogrammen also ständig gefragt, Updates zur Verfügung zu stellen, damit ihre Programme mit den aktuellen Kameramodellen zusammen arbeiten.

Ein Versuch, diesem Wirrwarr entgegen zu wirken, ist das von Adobe eingeführte DNG-Format, das "Digitale Negativ". In Qualität und Funktion entspricht es dem RAW-Format der Kamerahersteller, ist aber genormt und wird von vielen Bildbearbeitungsprogrammen "verstanden". Adobe empfiehlt (natürlich), alle RAW-Dateien im DNG-Format zu speichern und stellt dafür einen kostenfreien Konverter zur Verfügung.

Ich persönlich archiviere meine Bilder (noch) im RAW-Format, und speichere bearbeitete Bilder im TIFF-Format.

2.3 Speicherplatzbedarf

Zur Abschätzung des Speicherplatzbedarfs kann ich nur von meinen eigenen Daten ausgehen:

Ich habe im vergangenen Jahr (2006) rund 15.000 Fotos gemacht, anfangs nur als JPEG-Dateien, später zusätzlich im RAW-Format. Das ist ja gerade der Vorteil der Digitalkamera, dass man so viele Bilder machen kann, wie man will, und der Film nicht ausgerechnet im spannendsten Moment voll ist.
Gut, von diesen Bildern wird etwa die Hälfte bei der ersten Sichtung weggeworfen, aber es landen eben doch rund 8000 Bilder auf der Festplatte. Die Canon EOS 400d, die ich jetzt benutze, erzeugt pro Foto zwei Dateien (JPEG- und RAW-Format), die zusammen im Durchschnitt rund 15 MB groß sind. Die individuelle Größe ist vom Bildinhalt und seiner Komprimierbarkeit abhängig. Maximal 10% der Bilder lohnen die Nachbearbeitung, wobei dann deutlich größere Dateien anfallen, je nach Programm und Dateiformat 60-100 MB.
8000 x 15 MB sind 120 GB, dazu 800 x 100 MB = 80 GB, zusammen also im schlimmsten Fall rund 200 GB pro Jahr. In Datenträgern ausgedrückt sind das ca. 170 CDs oder 27 DVDs.

Noch weitaus sinnvoller ist natürlich rigoroses Ausmisten der Bilderbestände. Erfahrungsgemäß wird ein Großteil der Bilder sehr selten angeschaut, und viele davon sind unter Anwendung einigermaßen objektiver Maßstäbe verzichtbar. Nun gehört der Fotograf aber naturgemäß zur Gruppe der Jäger und Sammler, so dass ihm das Wegwerfen sehr schwer fällt.
Auch in meiner Bildersammlung sind noch viele Fotos, die ihren Speicherplatz eigentlich nicht wert sind. Und je länger sie im Bestand sind, desto schwieriger und aufwändiger wird das Aussortieren. Am leichtesten fällt es mir, solange die Bilder nicht älter als eine Woche sind.
Bewährt hat sich die Klassifizierung in "fotografisch wertvolle Bilder" und "Erinnerungsfotos". Von Letzteren brauche ich keine RAW-Dateien, den Platz spare ich mir. So komme ich auf maximal die Hälfte des im obigen Worst-Case-Szenario beschriebenen Platzbedarfs.

3 Datensicherung

Die übliche Konfiguration eines PCs für den Heimgebrauch enthält zwei Laufwerke, ein optisches und ein magnetisches.
Das optische Laufwerk ist heute ein DVD-ROM zum Lesen von CDs und DVDs oder ein Brenner zum Schreiben von CDs oder DVDs.
Das magnetische Laufwerk ist die Festplatte, auf der das Betriebssystem, die Programme und die Daten gespeichert sind. Dies ist das zentrale Gedächtnis, und im Falle einer Amnesie ist das ganze System unbrauchbar. Jedes andere Teil des Computers ist mit mehr oder weniger Aufwand ohne Datenverlust ersetzbar, die Festplatte nicht.

Das System selbst ist durch Neu-Installation von Betriebssystem und Anwendungsprogrammen mit Hilfe der Original-CDs wieder herstellbar, für die eigenen Daten jedoch gibt es keine Original-CD!

Technisch ist es kein Problem, einen defekten PC zu reparieren und wieder in Gang zu setzen, auch wenn das nicht jeder selbst machen kann. Auch können die Daten einer defekten Festplatte in der Regel gerettet werden, es gibt genügend Firmen, die mit dieser Dienstleistung ihr Geld verdienen. Ein Profi, für den der Verlust der Bilder den wirtschaftlichen Ruin darstellt, wird sicher einen solchen Dienst nutzen, für den Amateur lohnt sich das nicht. Ich könnte mir für das Geld eine komplette, neue Ausrüstung kaufen. Da investiere ich lieber 100,- € in eine zweite Festplatte.

Unter technischen und ökonomischen Gesichtspunkten scheint die Entscheidung für eine regelmäßige Datensicherung klar zu sein, wenn da nicht noch die Psychologie wäre…

Der Mensch hat ein gespaltenes Verhältnis zu Gefahren: Er fürchtet Risiken, die er nicht selbst beeinflussen kann, weitaus mehr als solche, bei denen er persönlich aktiv ist. So haben viel mehr Menschen Angst vor dem Fliegen als vor dem Autofahren, obwohl das Unfallrisiko im Straßenverkehr um Größenordnungen höher ist.
Und obwohl die Gefahr des Datenverlustes real ist, und die Frage nicht lautet, **ob** sondern **wann** der Katastrophenfall eintritt, handeln die meisten Menschen nach dem Motto "Mich wird's schon nicht treffen" und tun – nichts.

Wir werden sehen, dass es wirklich nur geringen Aufwands bedarf, seine Daten wirkungsvoll zu sichern, indem man Kopien davon anfertigt. Wie das am besten geschieht, hängt vom persönlichen Sicherheitsbedürfnis und der Bereitschaft, Aufwand dafür zu treiben, ab.

Betrachten wir als erstes die technischen Mittel, die uns als Privatanwendern zur Verfügung stehen, als da wären

- Optische Speichermedien,
- Interne und externe Festplatten,
- RAID-Systeme und
- Netzwerkserver.

Zu jeder der Alternativen werde ich Kosten und Aufwand betrachten und eine Einschätzung der Zuverlässigkeit versuchen."

Grundsätzlich ist zu sagen, dass der Aufwand zur Datensicherung wesentlich verringert wird, wenn die zu sichernden Daten an einem Ort zusammengefasst sind, sprich sich in einem Verzeichnis befinden. Bei Rechnern mit Windows XP als Betriebssystem bietet sich hierfür der Ordner "eigene Dateien" an, der vom System als Standardziel für selbst erstellt Dokumente vorgeschlagen wird.
Befinden sich alle Fotodateien im Ordner "eigene Dateien\Fotos", dort z.B. nach Jahren sortiert in Unterordnern 2006, 2005 usw., dann besteht die Sicherung dieser Daten lediglich darin, den Ordner "Fotos" zu kopieren – wohin auch immer.

3.1 CD- oder DVD-Brenner

In vielen PCs ist ein CD- oder DVD-Brenner bereits enthalten, so dass es eigentlich keine Ausrede gibt, nicht sofort eine Sicherheitskopie zu machen. Benötigt werden eigentlich nur noch CD- bzw. DVD-Rohlinge.
Bei dieser Strategie gibt es mehrere Probleme: Die Datenmenge und der damit verbundene Handhabungsaufwand, die fehlerfreie Speicherung und der langfristige Datenerhalt.

3.1.1 Kosten

Für viele PC-Benutzer ist die Sicherung ihrer Daten auf CD oder DVD die erste Wahl. Das benötigte Gerät ist vorhanden, Rohlinge sind überall erhältlich und preiswert, das Verfahren ist bekannt.
Bei geringen Datenmengen ist das sicher korrekt, wenn ich nur einmal im Jahr meine Korrespondenz sichern will, ist eine CD oder DVD genau das Richtige. Bei hinreichend großen Datenmengen läuft die Sache jedoch schnell aus dem Ruder, sowohl aufwandsmässig als auch finanziell.
Eine handelsübliche CD fasst ca. 700 MB, eine DVD 4,5 GB, bei Kosten von rund 20 bzw. 70 Ct pro Medium (Preise von Januar 2007 und qualitativ hochwertige Rohlinge vorausgesetzt). Pro GB Speicherplatz sind das etwa 10 bzw. 20 Ct. Wie viele Bilder darauf gesichert werden können, hängt von der Auflösung und der Art der Kamera ab. Ein Beispiel zur Abschätzung des Aufwands wurde in Kap. 2.3 bereits gegeben.
Geänderte Daten erfordern immer einen neuen Datenträger, Überschreiben ist nicht möglich!

3.1.2 Handhabung

Datensicherung auf CD ist nur bei geringen, auf DVD nur bei mittleren Datenmengen bequem. Sobald mehrere Datenträger erforderlich werden, wird die Handhabung zunehmend mühsamer, es ist viel Disziplin erforderlich, um nicht die Übersicht zu verlieren.
Optische Datenträger müssen vorsichtig behandelt und schonend gelagert werden – im Prinzip genauso wie Negative oder Dias.

3.1.3 Zuverlässigkeit

Vorteil der optischen Medien ist ihre einmalige Benutzbarkeit, d.h. es ist nicht möglich, Daten versehentlich zu löschen oder zu überschreiben. Auf der anderen Seite muss jede aktuell geänderte Datei zusätzlich gespeichert werden, benötigt also wieder Platz.
Nachteil ist, dass auf einen optischen Datenträger niemals fehlerfrei gespeichert wird. Normalerweise fällt das nicht auf, weil Fehlerkorrekturen mit abgespeichert werden. Wenn also Daten auf CD oder DVD geschrieben werden, sollte immer die Option "**geschriebene Daten überprüfen**" eingeschaltet sein, um sicherzustellen, dass die Daten korrekt auf der CD/DVD gelandet sind. Um späteren Schäden durch Kratzer und dergleichen vorzubeugen, sollte **jeder Datenträger zweimal gebrannt** werden, denn nichts ist ärgerlicher, als im Ernstfall festzustellen, dass ausgerechnet das beste Foto durch einen Kratzer unlesbar geworden ist.
Ein weiterer Nachteil ist die begrenzte Lebensdauer der Medien. CDs sagt man eine Lebensdauer von 10 Jahren nach, bei DVDs ist es weniger. Das sind jedoch statistische Werte unter optimalen Bedingungen, darauf verlassen möchte ich mich nicht. Es gibt Untersuchungen, die manchen Rohlingen eine Lebensdauer von weniger als einem Jahr bescheinigen, einige waren sogar direkt nach dem Brennen nicht mehr lesbar!
Ich würde die Daten regelmäßig überprüfen, d.h. wieder auf die Festplatte zurück kopieren und beim geringsten Anzeichen von Problemen (z.B. Pausen beim Einlesen) auf neue Datenträger brennen, spätestens aber nach fünf Jahren.

3.1.4 Fazit

Empfehlenswert nur bei geringen Datenmengen. Ich persönlich würde die Grenze bei etwa 10 Datenträgern ansetzen, also bei 7 bzw. 45 GB Datenvolumen.
Wer – wie ich – eine digitale Spiegelreflexkamera benutzt und RAW-Dateien speichert, stößt mit optischen Medien schnell an die Grenze des Sinnvollen. Ich müsste jedes Jahr über 30 € für mindestens 54 DVDs ausgeben und Disc-Jockey ist auch nicht mein Traumberuf.

3.2 Zweite Festplatte

Die meisten PCs können vier Laufwerke enthalten, moderne PCs mit Serial ATA Schnittstelle auch mehr. D.h. neben der primären Festplatte und dem optischen Laufwerk können noch mindestens zwei weitere Festplatten eingebaut werden, technisch ist die Aufrüstung also kein Problem.
Den mechanischen Einbau und den elektrischen Anschluss der Festplatte beschreibt das Handbuch des PCs. Nach dem nächsten Start erscheint dann ein weiteres Laufwerk im Explorer, das vor Gebrauch formatiert werden muss, empfehlenswert ist dabei die Schnellformatierung mit dem Dateisystem NTFS.
Sinnvollerweise wird dabei der Name der neuen Platte in "Backup" oder "Sicherung" geändert, so dass das neue Laufwerk schnell und eindeutig zu erkennen ist.

3.2.1 Kosten

Moderne Festplatten haben Kapazitäten von 200 bis 500 GB, reichen also in meinem Falle für etliche "Jahresproduktionen" aus. Zur Zeit (Januar 2007) bieten 250-GB-Platten das günstigste Preis-Leistungsverhältnis, die Kosten dafür betragen ca. 70 €, also rund 25 Ct pro GB.
Das ist nicht wesentlich teurer als die Speicherung auf optische Medien!

3.2.2 Handhabung

Befinden sich alle Fotodateien im Ordner "eigene Dateien\Fotos", dann besteht die Sicherung dieser Daten lediglich darin, den Ordner "Fotos" mit der Maus in das Laufwerk "Sicherung" zu ziehen und das Überschreiben bereits vorhandener Dateien zu gestatten.
Anschließend besitzt man ein vollständiges Duplikat des Bilderbestandes.
Der Vorgang ist beliebig wiederholbar.
Sollten die Bilddateien in verschiedenen Ordnern auf der Festplatte verteilt sein, würde ich zuerst einen zentralen Ordner "Fotos" anlegen und alle Ordner mit Bildern dorthin verschieben

Nachteil dieser einfachen Methode ist, dass jedes Mal **alle** Dateien kopiert werden, der Vorgang daher bei entsprechendem Datenvolumen Stunden dauern kann. Die Dauer lässt sich verkürzen, indem man nur die neu hinzugekommen Ordner kopiert, wobei man jedoch selbst darauf achten muss, keine Dateien oder Ordner auszulassen.
Einfacher und sicherer ist es daher, das Kopieren einem Programm zu übertragen, das für diese Aufgabe gemacht ist und nur die neuen und die veränderten Dateien kopiert. Solche Backup-Lösungen gibt es zuhauf, sowohl professionelle (teure) Programme als auch kostenlose Programme. Ich habe für meine persönlichen Bedürfnisse ein eigenes Programm geschrieben, das ich am Schluss auch kurz vorstelle.
Ein Nachteil der beliebigen Überschreibbarkeit der Daten ist natürlich, dass es genauso leicht möglich ist, Daten von der zweiten Festplatte zu löschen oder ein Original mit einer verkleinerten Kopie zu überschreiben. Es ist also Disziplin erforderlich und ein gewisses Maß an Verständnis für die Organisation der Dateien auf der Festplatte. Z.B. sollte man es sich zur festen Regel machen, nach der Bearbeitung niemals die Originaldatei zu überschreiben, sondern das Ergebnis unter einen veränderten Namen zu speichern.

3.2.3 Zuverlässigkeit

Moderne Festplatten sind für mehrjährigen Dauerbetrieb ausgelegt, können also durchaus als zuverlässiger Datenaufbewahrungsort gelten. Wie bereits gesagt, meine persönliche Erfahrung ist: alle sieben Jahre ein Ausfall.
Dennoch: Verlasse Dich nie darauf, dass die Festplatte, die jetzt seit Jahren zuverlässig ihren Dienst tut, auch morgen noch funktioniert!

3.2.4 Fazit

Zwei Festplatten mit identischem Datenbestand schützen bereits recht zuverlässig gegen elektrische oder mechanische Defekte des Datenträgers, und begrenzt gegen Anwenderfehler wie z.B. irrtümliches Überschreiben, weil zwei Aktionen für dasselbe Ergebnis nötig sind.
Schutz vor einer Katastrophe wie Diebstahl oder Brand bietet die Konstellation jedoch nicht, wird der PC zerstört oder gestohlen, sind wieder alle Daten futsch! Dieses Risiko lässt sich nur dadurch vermeiden, dass man die Backup-Daten an einem anderen Ort (im Büro, im Elternhaus etc.) aufbewahrt.

3.3 Externe Festplatten

Die externe Festplatte verhält sich am PC genauso wie eine interne. Ihr Vorteil gegenüber der internen Platte ist die leichte Transportierbarkeit, das oben genannte Diebstahls- oder Brandrisiko lässt sich damit einfach beherrschen.

3.3.1 Kosten

Die Kosten für eine externe Festplatte sind heute nur unwesentlich höher als die für eine interne Platte, auch der Speicherplatz liegt in derselben Größenordnung.
Die meisten externen Festplatten werden über USB angeschlossen, eine Standardschnittstelle für aktuelles Computerzubehör. Hier ist lediglich darauf zu achten, dass sowohl die Festplatte als auch der Anschluss am PC mit dem USB 2.0 Protokoll arbeiten, sonst dauert das Speichern viel zu lange.
Eine alternative Anschlussmöglichkeit ist Firewire, von der Leistung mit USB 2.0 vergleichbar, aber nicht so verbreitet.
Eine externe Festplatte ist zur Zeit ca. 20,- € teurer als eine gleich große, eingebaute Festplatte. Platten im Notebook-Format 2,5 Zoll sind teurer und haben eine geringere Kapazität, sind aber kleiner und leichter transportabel und benötigen in der Regel kein zusätzliches Netzgerät für die Stromversorgung. Hier kosten z.B. 120 GB rund 90,- €, also ca. 75 Ct pro GB.

3.3.2 Handhabung

Die externe Festplatte ist einfach transportabel und kann problemlos an jeden (Windows-)PC angeschlossen werden, und die Daten sind dort verfügbar.
Dies ist zugleich ihr Nachteil: Die externe Platte kann verloren gehen oder gestohlen werden, damit können also auch die wertvollen Daten in unbefugte Hände geraten.

Festplatten sind stoß empfindlich, besonders während des Betriebes. Es ist darauf zu achten, dass die Platte nicht anstößt oder gar fällt. Durch das Aufschlagen des Schreib-/Lesekopfes kann die empfindliche Plattenoberfläche oder der Kopf selbst beschädigt werden, und Datenverluste sind die sichere Folge. Hier sind die kleineren Notebook-Platten robuster, ihnen sagt man nach, dass sie einen Sturz aus 1m Höhe überstehen, aber mit meiner Platte werde ich das nicht ausprobieren.

3.3.3 Zuverlässigkeit

Hier gilt das zu den internen Festplatten Gesagte, wenn die externe Platte vor Stößen während des Betriebs bewahrt wird.

3.3.4 Fazit

Regelmäßiges Kopieren des Datenbestandes auf eine externe Festplatte bietet denselben Schutz vor einem Totalausfall der Platte wie die zweite, interne Platte. Wird sie räumlich getrennt aufbewahrt, kann sie zusätzlich Sicherheit gegen Verlust der Daten durch Naturkatastrophen oder Diebstahl gewähren.

3.4 RAID-Systeme

Ein RAID-System ist ein Verbund aus mehreren Festplatten, der für den PC ein einziges Laufwerk darstellt. Unter Datensicherungsaspekten ist hier nur die "Datenspiegelung" interessant, also der Parallelbetrieb zweier Platten, wobei das Betriebssystem selbst dafür sorgt, dass jede Datei in gleicher Weise auf beide Platten geschrieben wird.

3.4.1 Kosten

Wenn der PC bzw. sein Mainboard die RAID-Funktion unterstützen, entstehen an Kosten nur die für eine zweite Festplatte (die möglichst dieselbe Kapazität haben sollte wie die vorhandene). Hat der PC keine RAID-Funktion, fallen weitere Kosten für einen RAID-Controller in Form einer Einsteckkarte oder eine neues Mainboard an: je nach Leistungsfähigkeit 100 bis 500 €.

3.4.2 Handhabung

Ein RAID-System bietet die denkbar einfachste Handhabbarkeit: Es läuft alles automatisch, man muss lediglich von Zeit zu Zeit kontrollieren, ob noch beide Festplatten einwandfrei funktionieren, denn auch wenn eine defekt ist, funktioniert dank der Redundanz das System immer noch einwandfrei, es gibt nur kein Backup mehr!

3.4.3 Zuverlässigkeit

Dank seiner zwei Festplatten bietet das RAID-System dieselbe Zuverlässigkeit wie zwei einzelne Platten. Es schützt allerdings auch nur vor genau einem Schadensereignis, nämlich dem physikalischen Defekt einer Platte. Ein RAID-System bietet keinen Schutz gegen Anwenderfehler: Überschrieben oder gelöscht werden Dateien immer auf beiden Platten!

3.4.4 Fazit

Ein RAID-System ist Datensicherung für Faule, die ein nur geringes Sicherheitsbedürfnis haben. Wer mehr Einfluss auf Art und Umfang der Sicherung haben will, greift zur zweiten internen oder externen Festplatte.

3.5 Netzwerk-Server

Der Server ist ein zweiter (auch älterer) PC, der seine Festplatte(n) über das Netzwerk anderen PCs zur Verfügung stellt.
Erforderlich ist ein vollständiger PC einschließlich Betriebssystem (Windows oder Linux) und eine Netzwerkverbindung zum Arbeitsrechner, also mindestens ein Netzwerkanschluss in jedem Rechner (normalerweise vorhanden) und ein Verbindungskabel. Wer über einen Router (z.B. eine Fritz!Box) ins Internet geht, kann die Verbindung problemlos darüber herstellen.
Im einfachsten Fall (Windows-Betriebsystem) wird die Festplatte auf dem Server frei gegeben und verhält sich dann für den Arbeitsrechner wie ein weiteres Laufwerk. Wer die Möglichkeit hat, den Server in einem anderen Raum, z.B. im Keller unterzubringen, erreicht damit auch einen höheren Schutz vor Brandschäden und Diebstahl.
Mit entsprechender Software auf dem Server kann das Kopieren der Daten automatisiert werden, so dass die Daten des Arbeitsrechners regelmäßig gesichert werden, und auch nur die jeweils geänderten Daten.

3.5.1 Kosten

Die Einrichtung eines Servers, wenn nicht viele Arbeitsrechner zugleich auf die Daten zugreifen müssen, lohnt sich nur, wenn verwendbare Hardware (PC, Festplatte(n), Netzwerk) bereits vorhanden sind. Wenn der Server rund um die Uhr läuft, sind seine Stromkosten nicht mehr vernachlässigbar. Je nach Leistungsaufnahme können hier bis zu 100,- € pro Jahr zusammen kommen.
Einen Rechner eigens für diesen Zweck zu beschaffen (selbst wenn es ein Gebrauchter ist), lohnt sich für den Privatanwender nicht.

3.5.2 Handhabung

Die Installation eines Servers und die Automatisierung des Backups sind Spezialaufgaben und versierten PC-Anwendern vorbehalten. Für jemanden, der dies nicht täglich macht, sind einige Tage Arbeitsaufwand anzusetzen, entsprechendes Knowhow vorausgesetzt.
Ist der Server einmal eingerichtet, ist die Handhabung einfach, da das Kopieren der Daten automatisch geht.

3.5.3 Zuverlässigkeit

Die Wahrscheinlichkeit, dass Arbeitsrechner und Server zugleich ausfallen, ist um Größenordnungen geringer als der Ausfall eines PCs, ähnlich wie bei zwei Festplatten statt einer.
Setzt man für den Server – wie vorgeschlagen – gebrauchte Teile ein, wird die Ausfallwahrscheinlichkeit wegen des Verschleißes etwas höher, so dass die Verwendung von zwei Festplatten im Server empfehlenswert ist.

3.5.4 Fazit

Automatische Datensicherung durch einen Server erfordert entsprechendes Knowhow, das beim durchschnittlichen Digitalfotografen nicht vorausgesetzt werden kann. Auch sind die Kosten für einen Privatanwender unnötig hoch.

4 Datensicherheit

Eine weitere Möglichkeit des Datenverlustes ist, dass die wertvollen Bilddateien nicht zerstört werden, sondern in falsche Hände geraten. Eine möglicherweise noch verhängnisvollere Alternative, zumindest für den professionellen Fotografen.

Glücklicherweise ist auch dagegen ein Kraut gewachsen: die Datenverschlüsselung.
Und auch das ist gar nicht so kompliziert, wie wir gleich sehen werden.

4.1 Verschlüsselung mit Windows-Bordmitteln

Benutzer von Windows-XP besitzen bereits alles, was sie für die Datenverschlüsselung benötigen. Ein Rechtsklick auf den Ordner im Explorer reicht, und im Eigenschaftendialog kann unter "erweitert" die Verschlüsselung eingeschaltet werden.

Doch Vorsicht!
Ein Fallstrick ist bei dieser simplen Methode zu beachten: Die so verschlüsselten Daten können nur auf dem PC und unter der Benutzerkennung wieder gelesen werden, mit der sie auch verschlüsselt wurden. Auf einem anderen PC ist das Lesen nicht möglich, auch wenn man dort einen Benutzer mit demselben Namen anlegt. Sollte aus irgendeinem Grund eine Neu-Installation des Betriebssystems nötig werden, sind die Daten futsch, wenn nicht beizeiten der Schlüssel exportiert und an einen sicheren Ort kopiert wurde!
Für verschlüsselte Daten ist ein Backup also noch viel wichtiger als für unverschlüsselte, weil das Verlustrisiko größer ist.

4.1.1 Handhabung

Die Handhabung ist simpel, Verschlüsselung und Entschlüsselung macht das Betriebssystem automatisch im Hintergrund, der Benutzer bekommt davon gar nichts mit.
Das bedeutet aber auch, das die Daten für jeden zugänglich sind, der Zugang zum PC hat. Datenverluste durch Diebstahl oder Sabotage sind also nicht wesentlich erschwert.

4.1.2 Zuverlässigkeit

Der in Windows-XP verwendete Verschlüsselungsalgorithmus ist seit vielen Jahren bewährt, so dass sich die Speicherung in einem verschlüsselten Ordner nicht von der in einem normalen Ordner unterscheidet. Zur Sicherheit der Verschlüsselung kann ich keine Aussage machen, glaube aber, dass sie ausreicht, um die Daten vor normalen Menschen zu schützen, nicht jedoch vor dem CIA.
Das Betriebssystem denkt sich hier ein Passwort aus, so dass man die Sicherheit nicht durch die Auswahl eines entsprechenden Passworts beeinflussen kann.

4.2 Verschlüsselung mit TrueCrypt

Eine Alternative zu der windows-internen Funktion ist das Open-Source-Programm TrueCrypt, das frei verfügbar ist. Es arbeitet mit modernsten Verschlüsselungsalgorithmen und ich halte es für sicher und weitgehend unknackbar, weil sein Source-Code frei zugänglich ist und von Experten weltweit begutachtet wird.
Das Programm kann hier heruntergeladen werden: http://www.truecrypt.org/downloads.php
Eine deutschsprachige Beschreibung findet sich in der Wikipedia: http://de.wikipedia.org/wiki/TrueCrypt

4.2.1 Handhabung

Das Programm kann, muss aber nicht installiert werden. Meine externe Festplatte, die ich am Notebook benutze, enthält z.B. zwei Partitionen, eine unverschlüsselte, gerade groß genug, um dort das Programm TrueCrypt zu speichern, und eine große, verschlüsselte Partition für alle meine Daten.
So kann ich die Platte per USB an einen beliebigen Rechner anschließen, TrueCrypt starten, mein Passwort eingeben und habe dann Zugriff auf alle Daten. Die verschlüsselte Partition wird dann als weiteres Laufwerk eingebunden.
Lesen und Schreiben von Dateien erfolgt transparent im Hintergrund, so dass der Benutzer davon nichts merkt.

Die Sicherheit hängt hier ausschließlich vom verwendeten Passwort ab. Dabei gilt: je länger und komplizierter, desto sicherer! Nun sind lange, komplizierte Passwörter für Maschinen kein Problem, wohl aber für Menschen. Eine allgemein übliche und bewährte Methode ist, sich einen relativ einfach zu merkenden Satz auszudenken und dann die Anfangsbuchstaben der Wörter zu verwenden. Wenn man dabei Groß- und Kleinschreibung sowie die Satzzeichen mit berücksichtigt und Ziffern einstreut, indem man z.B. das Wort "ein" durch die Ziffer "1" ersetzt, kann man ein sehr sicheres Passwort erhalten.

Passwörter kürzer als 8 Zeichen oder ganze Wörter sind bei relativ geringem Aufwand auch mit einem handelsüblichen PC knackbar. Ein gutes Passwort sollte daher mindestens 12 Zeichen umfassen, Ziffern und Sonderzeichen enthalten und in keinem Wörterbuch vorkommen.
Wenn Sie den Namen Ihrer Katze als Passwort benutzen, kann jeder an Ihre Daten kommen, der Sie auch nur ein bisschen näher kennt!

4.2.2 Zuverlässigkeit

Ich benutze TrueCrypt seit Jahren und habe nie ein Problem damit gehabt.

Es ist empfehlenswert, nach dem Erstellen der verschlüsselten Partition den Partitions-Header zu sichern. Damit kann auch bei einer Beschädigung der Partition der Zugriff wieder hergestellt werden. Einzelheiten zur Vorgehensweise sind in der ausführlichen Programmbeschreibung nachzulesen.

Im Explorer ist die verschlüsselte Partition auch als normales Laufwerk zu sehen, hier als „Lokaler Datenträger (W:)“. Nach Eingabe des Passwortes erscheint das zusätzliche Laufwerk „Mobil (M:)“:

Das Laufwerk W: darf **niemals formatiert** werden, damit würde das verschlüsselte Laufwerk M: zerstört!

5 Datenwiederherstellung

Datensicherung beherrschen wir nun, aber was, wenn tatsächlich der Ernstfall eintritt und die Festplatte mit den Fotos den Geist aufgibt? Wie kriegt man seine Dateien zurück?

Im Grunde ist es einfach, man muss nur eine neue Festplatte kaufen, sie gegen die alte austauschen und die Daten von der Backup-Platte dorthin kopieren.
Und genau hier liegt das größte Risiko in der Datensicherung. Rein statistisch passieren die meisten Katastrophen, die zum totalen Datenverlust führen, beim Zurückspielen der Sicherung.

Der kritische Fall ist dann gegeben, wenn der Datenbestand nur noch auf dem Backupmedium vorhanden ist. Dann gibt es nämlich keine Sicherungskopie mehr, auf die man notfalls zurückgreifen könnte!

5.1 Problem 1: Identifizieren der Festplatte

Sie öffnen den PC durch Entfernen der Seitenwand und sehen zwei Festplatten, ähnlich wie die, die Sie als Ersatz gekauft haben. Welche der beiden ist nun diejenige, die ausgetauscht werden muss? Rein äußerlich können Sie das nicht entscheiden, weil von Typ und Bauform nur selten auf den Inhalt geschlossen werden kann. Die sichere Methode ist, von einer der beiden Platten das Datenkabel (das breite, flache – das mit den roten, schwarzen und gelben Drähten dient der Stromversorgung) abziehen und dann den PC einzuschalten. Startet der PC ganz normal und es fehlt im Explorer nur das Datenlaufwerk, dann haben Sie die richtige Festplatte erwischt. Bleibt der Bildschirm dunkel und der PC startet nicht, dann war das die Systemplatte und die andere ist die richtige.

Nun wird die defekte Platte ausgebaut und durch die neu gekaufte ersetzt. Sie wird genauso angeschlossen wie ihre Vorgängerin.

5.2 Problem 2: Identifizieren des Laufwerks

Festplatte und Laufwerk ist nicht dasselbe: Die Festplatte ist das Teil, das Sie in die Hand nehmen können und auf dem die Daten physikalisch gespeichert werden, das Laufwerk hingegen ist eine logische Einteilung des verfügbaren Speicherplatzes durch das Betriebssystem.

In unserem Beispiel-PC stecken zwei Festplatten, aber im Explorer werden drei Laufwerke angezeigt, weil die erste Festplatte in zwei Partitionen unterteilt ist, die jeweils ein logisches Laufwerk enthalten.

Angenommen, das Laufwerk mit den Daten hat den Laufwerksbuchstaben D und die Sicherung ist auf Laufwerk E, und Laufwerk D fällt aus. Sie kaufen eine neue Festplatte, bauen sie in den Rechner ein und starten ihn. Einen fabrikfrische Festplatte ist komplett leer, muss also vor Gebrauch zuerst formatiert werden. Kein Problem, ein Rechtsklick auf das Laufwerk im Explorer öffnet das Kontextmenü, welches den Menüpunkt "Formatieren" anbietet.
Allerdings hat der PC nun dem Sicherungslaufwerk den Buchstaben D zugewiesen, und das neue Laufwerk E genannt, weil es noch nicht formatiert ist. Windows hat nun mal die Eigenart, Laufwerksbuchstaben scheinbar willkürlich zuzuordnen. Sie wählen also Laufwerk D aus und formatieren es, in dem guten Glauben, es sei das neue Datenlaufwerk. **In Wirklichkeit vernichten Sie gerade Ihr Backup!**

Genau deswegen empfehle ich, wichtige Daten **dreimal** zu speichern. Denn diese Verwechslung passiert auch erfahrenen PC-Benutzern. Getreu Murphy's Gesetz: Ein Fehler passiert immer genau dann, wenn der größte Schaden angerichtet werden kann.

Es gibt zwar auch Tools, die die Formatierung rückgängig machen können, aber das ist wieder mit Kosten und Aufwand verbunden.

Gerade beim Wiederherstellen der wichtigen Dateien ist höchste Konzentration und Sorgfalt erforderlich. Lieber dreimal kontrollieren, ob das, was man gerade zu tun beabsichtigt, auch wirklich korrekt ist und zum gewünschten Ergebnis führen wird. Also z.B. vor dem Formatieren überprüfen, welche Daten das zu formatierende Laufwerk enthält, und ob das wirklich verzichtbare Daten sind.

6 Meine Lösung

Meine Rechner hat zwei interne Festplatten: Die erste enthält die Partition für das Betriebssystem (Windows XP) und - da die Platte damit bei weitem nicht ausgelastet ist - eine Backuppartition, auf der zweiten Platte ist die Datenpartition. Damit sind System und installierte Programme auf Laufwerk C: sauber von den Daten auf Laufwerk D: getrennt, und ich kann beide unabhängig voneinander sichern.
Den Ordner "eigene Dateien" habe ich auf D:\ geändert, das geht einfach über den Eigenschaftsdialog des Ordners im Explorer.

6.1 System-Backup

Für die Systempartition wird am besten ein Image-Programm eingesetzt wie beispielsweise Norton Ghost, DriveImage oder Acronis TrueImage. Das Backup der Systempartition muss auf dem Datenlaufwerk (oder extern) gespeichert werden, da es nur auf einer anderen Festplatte Sinn macht. Falls die erste Festplatte aufgrund eines Defekts ausfällt, kann durch Zurückspielen des Images auf eine Ersatzplatte das System schnell wieder lauffähig gemacht werden. Lebensnotwendig ist diese Sicherung nicht, man kann das System auch von den Originaldatenträgern wieder neu installieren, sie spart allerdings eine Menge Zeit.
Auch hier ist das doppelte Backup auf eine weitere Platte oder auf eine DVD sehr empfehlenswert. Die vom Image-Programm erzeugte Datei kann wie jede andere auch kopiert oder gebrannt werden, wenn sie nicht zu groß ist. Falls sie gerade nicht auf eine DVD passen sollte, kann in der Regel im Image-Programm ein höherer Kompressionsgrad gewählt werden.

6.2 Daten-Backup

Für die Sicherung der Daten gibt es Backup-Lösungen wie Sand am Meer, wobei man auch mit den Windows-Bordmitteln zurecht kommen kann: zur Not kann das Foto-Verzeichnis mit dem Windows-Explorer kopiert werden. Für die erstmalige Kopie ist das gar keine schlechte Lösung, nur ab dem zweiten Mal wird es zeitaufwendig, den der Explorer kann nur wieder alles kopieren (und überschreiben), er kann sich nicht auf die neuen und geänderten Dateien beschränken. Die Aktion ist daher immer ein Komplett-Backup, die bei hinreichender Datenmenge Stunden dauern kann.

6.3 PS_Backup

Da ich unter der Vielzahl der angebotenen Backup-Programme keines gefunden habe, was genau auf meine Bedürfnisse passte, und ich Programmierer bin, habe ich mein eigenes Backup-Programm geschrieben. Es erfüllt sowohl die Anforderungen, die ich als Software-Entwickler an ein solches Programm stelle, als auch die des Fotografen. Das Programm heißt **PS_Backup** und kann auf meiner Homepage (http://www.p3so.de/p/bak_page.html) herunter geladen werden.

Backup-Aufgaben werden als "Jobs" definiert, die mehrere Quellverzeichnisse und ein Zielverzeichnis enthalten können und durch den Backup-Modus und den Ausführungszeitpunkt beschrieben sind.

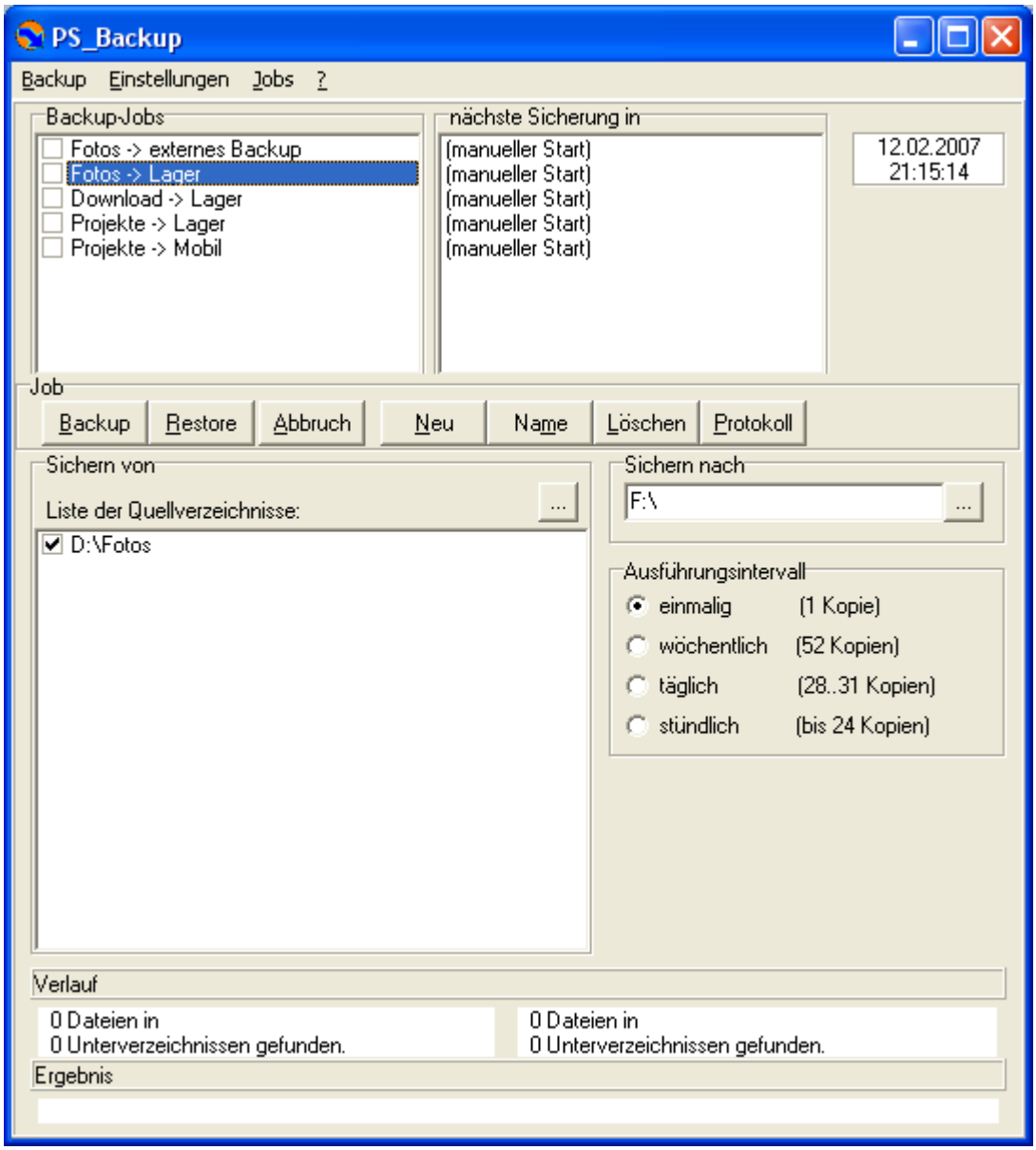
Der Backup-Modus kann gewählt werden als

- manuell (Start durch Anklicken der Schaltfläche "Backup")
- stündlich (automatischer Start innerhalb der Grenzen "von - bis")
- täglich (automatischer Start um hh:mm:ss Uhr)
- wöchentlich (automatischer Start am dd.mm.jjjj um hh:mm:ss Uhr)

Beim Start des Jobs wird eine Liste aller Dateien der Quellverzeichnisse erstellt und mit der Dateiliste aus dem Zielverzeichnis verglichen. Alles, was neu ist, wird kopiert, alles, was jünger ist, wird ersetzt. Im Zielverzeichnis befindet sich so stets eine aktuelle und vollständige Kopie der Quelle(n).

Kopieren in der umgekehrten Richtung ist mit der "Restore"-Schaltfläche möglich. Ich mache das aber lieber direkt mit dem Windows-Explorer, da habe ich mehr Kontrolle darüber, was zurück kopiert wird.

Alle Aktionen des Programms werden protokolliert.



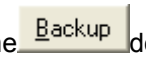
Das Programm wird als gezippte Datei heruntergeladen. Das Archiv enthält lediglich die Programmdatei "PS_Backup.exe", die in einen beliebigen Ordner entpackt werden kann und ohne Installation benutzt werden kann.

Zu Beginn ist die Jobliste leer. Mit der Schaltfläche Neu wird ein Job angelegt, der dann "Job 1" heißt.

Der neue Job bekommt mittels der Schaltfläche Name eine aussagekräftigere Bezeichnung, z.B. "Fotos -> internes Backup".

Um die Liste der Quellverzeichnisse zu füllen, kann die Schaltfläche ... benutzt werden, die den Verzeichnisauswahldialog von Windows öffnet. Damit das Verzeichnis beim Backup auch berücksichtigt wird, muss noch das Häkchen gesetzt werden.

In das Feld "Sichern nach" wird auf die gleiche Weise das Zielverzeichnis (in meinem Fall die Backup-Partition auf der ersten Festplatte) ausgewählt.

Und nun kann mit der Schaltfläche 

der Kopiervorgang gestartet werden.
Das Programm beginnt damit, die Struktur des (ersten) Quellverzeichnisses mit allen Dateien einzulesen, anschließend wird die Liste der im Zielverzeichnis bereits vorhandenen Dateien erstellt, die bei der ersten Ausführung wahrscheinlich leer ist.
Dann werden die beiden Listen verglichen und alle Dateien, die auf der Zielseite fehlen oder auf der Quellseite jüngeren Datums sind, kopiert. Beim ersten Lauf werden damit natürlich alle Dateien kopiert. Während des Kopierens wird ein Protokoll aller Aktionen angezeigt, das auch gespeichert werden kann.

Beim Beenden des Programms werden die Jobs und ihre Einstellungen automatisch gespeichert und stehen beim nächsten Start wieder zur Verfügung. Dann genügt es, wieder auf **Backup** zu klicken (und ggf. vorher den Job auszuwählen), und das Programm vergleicht wieder die beiden Dateilisten und kopiert, was neu(er) ist.
Das ist der Vorteil eines Backup-Programms gegenüber der einfachen Lösung mit dem Windows-Explorer: Es spart bei nachfolgenden Backups sehr viel Zeit, weil nur die Änderungen übertragen werden.

Eines sei allerdings nicht verschwiegen: **Ich übernehme keinerlei Garantie für die korrekte Funktion des Programms, der Einsatz erfolgt auf eigene Verantwortung.**
Ich nutze das Programm zwar schon seit fast einem Jahr ohne nennenswerte Probleme auf drei Rechnern, aber Benutzer von Programmen haben immer schon eine unglaubliche Phantasie in der Verwendung von Software bewiesen und Probleme aufgedeckt, an die der Programmierer in seinen schlimmsten Alpträumen nicht gedacht hätte...
Und ein noch nicht gelöstes Problem ist der Umgang mit schreibgeschützten Dateien: Das Programm kann Dateien, die im Zielverzeichnis schreibgeschützt sind, nicht überschreiben. Wenn es mir wichtig wird, werde ich das ändern, normalerweise habe ich keine schreibgeschützten Dateien.

6.4 Externe Festplatte(n)

Um eine zweite, räumlich getrennte Sicherungskopie meiner Daten machen zu können, habe ich eine weitere, externe Festplatte, die per USB angeschlossen wird.

Es handelt sich dabei um eine (ältere) Festplatte im 3,5-Zoll-Format, wie sie auch im Rechner eingebaut sind.
Immer wenn Fotos hinzugekommen sind oder bearbeitet wurden, schließe ich diese Platte an den Rechner an und lasse den zugehörigen Backup-Job laufen, der meine wichtigen Daten auf Laufwerk X: (X wie extern) kopiert. Die Platte bewahre ich in meinem Büro in der Firma auf. Selbst wenn das Haus abbrennt, habe ich meine Fotos immer noch sicher!
Und damit kein Unbefugter an die Daten kommt, ist die Platte mittels TrueCrypt verschlüsselt.

Eine weitere externe Festplatte dient der mobilen Datensicherung des Notebooks. Dies ist eine Platte im 2,5-Zoll-Format, sie ist also klein und leicht zu transportieren. Und damit auch leicht zu verlieren! Daher ist die Partition auf dieser Platte ebenfalls mit TrueCrypt verschlüsselt, genauso wie das Datenlaufwerk im Notebook selbst.
Da die Platte deutlich kleiner ist als die internen Platten, kopiere ich hierauf keine Fotos, sondern nur Schriftstücke und Programmquelltexte.

7 Zusammenfassung

Ich hoffe, mit diesen Ausführung die Motivation zur Datensicherung ein wenig gesteigert zu haben.

Denken Sie daran: **Es ist nicht die Frage, ob eine Festplatte ausfällt, sondern nur, wann!**

Meine Empfehlung ist:

Den Datenbestand (und nur den, nicht Programme oder Betriebssystem) regelmäßig, am besten automatisiert, auf zwei weitere Festplatten zu speichern, so dass alle Daten dreimal vorhanden sind. Festplatten sind nach dem derzeitigen Stand der Technik die zuverlässigsten Speichermedien.

Mindestens eine der beiden Platten sollte eine externe sein und an einem anderen Ort aufbewahrt werden. Wenn beide Backup-Medien externe Platten sind, dann sollten sie regelmäßig getauscht werden, damit der Datenbestand außer Haus nicht zu sehr veraltet.

Sinnvollerweise werden externe Festplatten verschlüsselt, da sie außer Haus aufbewahrt werden.