2 Risiken

2.1 Die Festplatte ist defekt

Die meisten Festplatten werden nach wenigen Jahren zusammen mit dem Computer entsorgt oder gegen größere Platten ausgetauscht. Deshalb werden Festplatten von ihren Herstellern nicht für einen langjährigen Einsatz konzipiert. Je nach Benutzung (24 oder 8 Stunden täglich) hält eine Festplatte zwei bis fünf Jahre mit erträglicher Wahrscheinlichkeit durch, stromsparende „grüne" Festplatten etwas länger.

Selbst wenn Sie die Warnzeichen für einen bevorstehenden Ausfall kennen und beachten, eines Tages wird es passieren: Die Festplatte geht kaputt.

Stellen Sie sich einmal vor: Jetzt, in diesem Moment, geht Ihre Festplatte unrettbar kaputt. Wie groß wäre der Schaden? Wie wertvoll sind Ihre Daten?

2.1.1 Verlust der Daten

Beginnen wir mit den Daten, die jeder hat:

- Haben Sie alle Zugangsdaten (DSL, E-Mail, eBay, Messenger, Chat, Facebook, ...) aufgeschrieben? Auch die Daten von allen Online-Shops, in denen Sie vielleicht wieder einmal einkaufen wollen? Auf Papier oder nur in einer Datei auf der nunmehr defekten Festplatte? Oder in einem „Password-Safe", den Sie nicht mehr öffnen können?
- Wo sind Ihre E-Mails gespeichert? Auf Ihrem PC oder auf dem Server des Providers? Werden sie dort nach drei Monaten automatisch gelöscht? Vielleicht sind auch E-Mails dabei, mit denen Sie Passworte und Zugangskennungen erhalten haben. Habe Sie diese alle ausgedruckt und abgeheftet?
- Wie viele Einträge hat Ihr E-Mail-Adressbuch? Wie sieht es mit Skype- und Chatpartnern aus? Wie aufwändig wäre es, diese Adressen wiederzubeschaffen?
- Wie viele Links hat Ihre Favoritenliste? Wie lange würde es dauern, alle oder wenigstens die wichtigsten davon wiederzufinden?
- Benutzen Sie ein Lohnsteuerprogramm? Wie lange würden Sie brauchen, die Daten ein zweites Mal zu erfassen?
- Wie bitter wäre es für Sie, Fotos und Filme von den Urlaubsreisen der letzten Jahre, von der Hochzeit und anderen Familienfeiern und von den heranwachsenden Kindern zu verlieren? Selbst wenn die Originale aller Fotos auf irgendwelchen CDs oder DVDs zu finden sind (und diese noch lesbar sind): Wie lange würde es dauern, sie auf die Festplatte zu kopieren, zu ordnen, misslungene Aufnahmen zu löschen und auf der Seite liegende Aufnahmen hochkant zu drehen?

Eine geübte Schreibkraft braucht für die Neueingabe einer eng beschriebenen DIN A4-Seite etwa 15 Minuten. Auf eine Diskette (1,44 MB) passen etwa 700 Seiten, was 22 Arbeitstagen zu je 8 Stunden entspricht. Auf einen winzigen USB-Memory-Stick von 1 GB passen etwa 500 000 Seiten (60 Arbeitsjahre). Vermutlich ist ein mehr oder weniger großer Teil der alten Daten entbehrlich, aber bestimmt gibt es auch Daten, auf die Sie nicht gern verzichten würden.

Eine Sicherheitskopie für eine übliche Datenmenge zu erstellen kostet Sie weniger als einen Euro und das erste Mal weniger als eine Stunde Zeit. Bei einem wohldurchdachten Konzept dauert jede nachfolgende Sicherung nur einige Minuten.

2.1.2 Verlust des Betriebssystems

Das Betriebssystem neu installieren zu müssen ist eine langwierige Arbeit. Nicht nur Windows muss installiert werden, sondern auch alle Treiber, alle Updates und alle Anwendungen. Sind Ihre Installations-CDs vollständig und in gutem Zustand? Haben Sie die Seriennummern für alle Programme, die Zugangsdaten und die Lizenzen? Vermutlich haben Sie aktuelle Treiber und zahlreiche nützliche Programme im Internet gefunden und installiert. Haben Sie deren Web-Adressen griffbereit? Falls Sie Abonnements von Antiviren- und anderen Programmen über das Internet verlängert haben, wie können Sie die Zahlung nachweisen?

Eine Schätzung: Wie aufwändig ist eine Neuinstallation?

1,5 h Alle Daten auf DVD o. Ä. sichern, ohne etwas zu vergessen. Beachten Sie: Sowohl die „Datensicherung mit 18 Klicks“ als auch die „Datensicherung mit Windows-Bordmitteln“ sichern nur ausgewählte Dateien, nicht die gesamte Festplatte. Die wichtigsten Daten sollten Sie zweimal sichern (die DVD mit Ihrer Datensicherung könnte sich als fehlerhaft herausstellen), am allerbesten mit zwei verschiedenen Verfahren sichern (DVD brennen plus externe Festplatte). Falls Sie keine externe Festplatte haben und deshalb beide Sicherungen nur auf DVD brennen können, sollten Sie Rohlinge verschiedener Fabrikate verwenden. Mindestens eine der gebrannten DVDs sollten Sie stichprobenartig prüfen:

- Sind Ihre wichtigsten Dateien auf der DVD vorhanden? Überprüfen Sie das Inhaltsverzeichnis!
- Klicken Sie einige Ihrer Dateien an. Lassen sie sich öffnen?

0,5 h Alle Passwörter (T-Online, Ebay, E-Mail, Musicload, ...) heraussuchen. Wenn Sie ein Passwort nicht wissen und Sie das Programm noch mit dem im PC gespeicherten Passwort starten können, wechseln Sie vorsorglich das Passwort und notieren Sie das neue.

0,5 h Zu jedem Programm die Installations-CD und die Seriennummer (den „Product Key“) heraussuchen.

0,5 h Alle Treiber auf einem USB-Stick o. Ä. bereitlegen. Am wichtigsten ist der Treiber für die Netzwerkkarte, damit Sie mit dem neuen Windows ins Internet kommen, um nach weiteren Treibern suchen zu können.

1,0 h Die Partition mit dem alten Windows löschen, Windows installieren und Treiber für Chipsatz, Sound, Netzwerk, Grafikkarte u. a. installieren.

0,5 h Internet-Zugang einrichten.

1,0 h Alle Patches und Sicherheitsupdates herunterladen und installieren, das können mehr als hundert sein. Wenn der Internetzugang über UMTS erfolgt, wird dabei wahrscheinlich das monatliche Download-Kontingent ausgeschöpft und der Download dauert sehr viele Stunden.

5,0 h für Installation, Freischaltung, Updates, benutzerdefinierte Anpassung und Einfügen der gesicherten Daten bei einer Minimalausstattung von zehn Programmen, z. B. Antivirenprogramm, Browser, E-Mail, Brenner, DVD-Player, Adobe Reader, Flash Player, Bildbearbeitungs- oder Bildanzeigeprogramm, Office-Paket oder Schreibprogramm, Packprogramm.

1,0 h für das Anlernen des Spam-Filters und der Software-Firewall, soweit vorhanden.

Das sind mindestens zwölf Stunden, und Sie haben bestimmt noch mehr als nur zehn Programme. Sie werden noch tagelang mit kleinen Nachbesserungen und individuellen Anpassungen zu tun haben. Und wenn Sie nicht ganz genau wissen, wie Sie vorgehen müssen, kann es noch sehr viel länger dauern.

Multiplizieren Sie die Stundenzahl mit dem Stundensatz Ihres Computerexperten, -händlers oder Ihrem eigenen Stundensatz, um den materiellen Schaden abzuschätzen.

2.2 UNTERSCHIED ZWISCHEN DATEN- UND SYSTEMSICHERUNG

Mit einem Backup können zwei verschiedene Ziele erreicht werden, die genau unterschieden werden müssen.

- Eine Systemsicherung bringt Ihren PC schnell wieder zum Laufen, wenn Windows beschädigt ist.
- Die Datensicherung sichert die Ergebnisse Ihrer Arbeit.

2.2.1 Systemsicherung

Eine **System**sicherung ermöglicht eine schnelle Wiederherstellung der Arbeitsfähigkeit, wenn das Betriebssystem Schaden genommen hat oder die Festplatte defekt ist. Nebenbei werden dabei wahrscheinlich einige Ihrer Daten gesichert, doch das ist zweitrangig (das ist die Aufgabe der **Daten**sicherung). Um ein solches Backup zu erzeugen, muss ein genaues Abbild des gesamten Festplatteninhaltes (ein Disk Image) erstellt werden. Dabei sind vier Probleme zu überwinden.

1. Einige Dateien sind ständig in Benutzung, als Beispiele seien die Benutzereinstellungen, die Registry und die Auslagerungsdatei genannt. Es ist nicht ohne weiteres möglich, diese Dateien zu kopieren, und mit den Windows-Bordmitteln gelingt das schon gar nicht.
2. Auch wenn Sie gerade nichts tun – Windows ist nie untätig. Die Speicherbelegung wird optimiert (Auslagerungsdatei), der Suchindex wird aktualisiert, einige Programme suchen im Internet nach Updates und manche Anwenderprogramme speichern alle paar Minuten ihren aktuellen Zustand, um nach einem eventuellen Absturz fast verlustfrei fortsetzen zu können. Das bedeutet: Während eine Systemsicherung läuft, werden immer wieder Dateien verändert, darunter auch einige der bereits kopierten Dateien. Im Ergebnis enthält die Systemsicherung einige Bestandteile, die nicht zueinander passen.
3. Es würde nicht genügen, alle Dateien zu kopieren und sie bei Bedarf zurückzukopieren. Einige Dateien müssen sich an einer präzise definierten Stelle befinden, sonst startet das Betriebssystem nicht. Der Windows-Explorer und andere Kopierprogramme können das nicht, sie kopieren die Dateien irgendwohin, wo gerade Platz frei ist.
4. Das Zurückkopieren muss natürlich auch dann möglich sein, wenn Windows nicht mehr startet.

Daraus ergeben sich drei Anforderungen an die Software:

1. Das Sichern und Zurückkopieren muss nicht Datei für Datei, sondern Spur für Spur, Sektor für Sektor erfolgen. Was ursprünglich im Sektor 1 der Festplatte war, muss nach Sektor 1 zurück.
2. Das Backup-Programm muss von CD startfähig sein. Dadurch werden die Probleme mit ständig benutzten und geänderten Dateien gelöst: Weil Windows weder beim Backup noch zum Restore gestartet werden muss, bleiben alle Dateien der Festplatte unbenutzt.
3. Aus 1. und 2. folgt: Das Backup-Programm muss mit jeder gängiger Hardware zurechtkommen, denn es kann nicht auf die Treiberunterstützung des Betriebssystems zurückgreifen. Deshalb sollte das Disk-ImageProgramm nicht älter sein als Ihre Computerhardware. Es passiert nicht selten, dass eine Image-Software meldet, es wären keine Festplatten vorhanden. Vor allem bei Notebooks kommen mitunter Festplattencontroller zum Einsatz, die recht exotische Treiber benötigen.

Programme, die mit diesen Anforderungen zurechtkommen, werden als Image-Programme bezeichnet. Mehr dazu in einem späteren Kapitel.

Für die Systemsicherung wird in der Regel ein Backup-Medium mit hoher Kapazität benötigt, am besten ist eine externe Festplatte geeignet. Windows 7, 8, 10 und Vista plus einige Anwendungen belegen etwa 20 GB und mehr. Zwar können die meisten Backup-Programme die Daten komprimieren, wodurch der Speicherbedarf um etwa 30 % sinkt, aber das ist immer noch zu viel, wenn eine Sicherung auf DVD erfolgen soll. Eine Systemsicherung, für die mehrere DVD benötigt werden, ist deshalb relativ zeitaufwändig.

2.2.2 Datensicherung

Eine **Daten** sicherung bewahrt **die Ergebnisse Ihrer Arbeit** vor Verlust: Dokumente, Fotos, Musik und Videos. Die einzelnen Dateien sind meist nicht groß: Auf einem Gigabyte Speicherplatz kann man etwa 500 Fotos, 250 MP3-Dateien oder den Inhalt eines 10 m hohen Bücherstapels unterbringen. Bei vernünftiger Planung reicht die Speicherkapazität einer CD oder DVD für ein Daten-Backup aus, vielleicht genügt sogar ein USB-Speicherstick. Je öfter die Sicherung erfolgt, desto weniger Arbeit haben Sie bei der Wiederherstellung nach einem Verlust. Wenn Ihre letzte Datensicherung beispielsweise einen Monat zurückliegt, werden Sie nach einem Verlustfall die Arbeit des letzten Monats noch einmal erarbeiten müssen oder darauf verzichten müssen. Eine häufige Sicherung ist deshalb ratsam.

2.2.3 Vergleich

Eine gute Datensicherung ist noch wichtiger als die Systemsicherung. Wenn Sie kein Systembackup haben, können Sie die Computerinstallation auch ohne jedes Backup wiederherstellen, durch Wiederaufspielen der Installationsmedien. Sie müssen Windows und alle Ihre Anwendungen von Grund auf neu installieren, Updates installieren und das System an Ihre Bedürfnisse anpassen. Das dauert einen ganzen Arbeitstag oder mehr. Aber eine Katastrophe ist das nicht. Außer einer großen Menge Ihrer Arbeitszeit geht nichts verloren. Deshalb braucht eine Systemsicherung nur in größeren Abständen durchgeführt werden, vorzugsweise nach der Installation neuer Programme oder nach größeren Änderungen am Betriebssystem.

Wenn Sie jedoch keine **Daten**sicherung haben, ist Ihre Arbeit verloren.

Wenn das Betriebssystem beschädigt oder infiziert ist und Sie eine Systemsicherung haben, können Sie den PC schon nach einer halben Stunde wieder benutzen. Wenn Sie Daten auf der Systempartition haben, die Sie seit dem letzten Systembackup verändert haben, dauert es nur wenig länger: Sie sichern schnell noch die kürzlich veränderten Daten, stellen das Betriebssystem samt der alten Daten wieder her und kopieren dann die neuesten Daten zurück.

Viele Komplettsysteme und fast alle Notebooks werden mit einer Systemsicherung ausgestattet: Mit einer „Recovery-DVD“ oder einer Recovery-Partition. Bei vielen Komplettsystemen werden Sie nach der ersten Inbetriebnahme dazu aufgefordert, diese DVD selbst zu erstellen. Es handelt sich dabei um ein Image, mit dem Sie den Neuzustand des Geräts wiederherstellen können. Wobei „Neuzustand“ logischerweise bedeutet, dass alle Ihre Daten rettungslos verloren sind.

Die aufwändige Sicherung des Betriebssystems nur selten durchzuführen und dafür die Daten häufiger zu sichern – das wäre optimal. Dafür ist es aber zwingend notwendig, Betriebssystem und Daten zu trennen. Das wäre mit zwei Festplatten möglich – eine für Betriebssystem und Programme, die möglichst keine Daten enthält, und eine andere Festplatte nur für Daten. Billiger ist es, eine einzige Festplatte in mindestens zwei Partitionen aufzuteilen, mehr dazu im Kapitel über Partitionen.

Für die Systemsicherung ist ein Image-Programm am besten geeignet. Doch für die Sicherung der Daten ist ein Image wenig geeignet: Selbst wenn nur eine einzelne Datei aus einem Image benötigt wird, muss man bei vielen Image-Programmen das komplette Image irgendwohin auspacken, um an einzelne Dateien heranzukommen. „Acronis True Image“ ist eine löbliche Ausnahme: Damit kann man einzelne Dateien oder Ordner aus einem Archiv extrahieren, ohne das ganze Archiv auspacken zu müssen.

Doch trotzdem ist ein Image nicht die beste Lösung für die Sicherung der Daten. Die gesamte Partition sichern, auch wenn die meisten Dateien seit längerem unverändert sind, ist zeit- und speicherplatzaufwändig. Nötig ist eine Backup-Software, die nur die veränderten Dateien sichert, aber das möglichst oft: Eine „Version-Backup-Software“. Es gibt keine Software, die beide Aufgaben optimal löst.

2.3 Welche Gefahren drohen Ihren Daten

2.3.1 Risikofaktor Mensch

- Bedienfehler (versehentliches Löschen einer Datei oder einer Dateiversion),
- Fehler aus mangelndem Wissen über Computer und Software,
- falsche Anwendung von Hilfsprogrammen, vor allem von Partitionierungs-Tools,
- Nichtbeachtung von Warnhinweisen,
- Nichtbeachtung der Garantiebedingungen bzw. AGB (viele Reparaturbetriebe stellen routinemäßig den Verkaufszustand wieder her und löschen dabei Ihre Daten),
- Diebe räumen Ihre Wohnung aus,
- Sie vergessen das Notebook im Taxi oder in der Bahn,
- der Memory-Stick ist nicht mehr aufzufinden sowie
- „Schabernack“ oder Vandalismus durch Kinder, Kollegen oder Gäste.

Der Mensch (als Bediener oder als Programmierer von nützlicher oder schädlicher Software) verursacht statistisch etwa 85 % aller Schäden. Es bleiben nur 15 %, die auf die technische Umwelt (z. B. Festplattenschaden) sowie Elementarschäden entfallen.

2.3.2 Risikofaktor Software

- Fehler im Betriebssystem und Sicherheitslücken,
- fehlerhafte oder unpassende Treiber,
- Datenverlust durch ein Update oder durch die Installation eines Servicepacks,
- Viren, Würmer, Trojaner, Datendiebstahl (Phishing) und Hacker-Attacken,
- inkompatible Programme und veraltete Hilfsprogramme. Wenn man zu einem neueren Betriebssystem wechselt, können die Tools von der Vorgängerversion, wenn sie nicht upgedatet werden, ein erhebliches Risiko darstellen.

Dazu ein Beispiel. Meine Festplatte war zu klein geworden und ich hatte mir eine große 2000 GB Festplatte zugelegt. Hinter einer 200 GB Partition für das Betriebssystem hatte ich eine erweiterte Partition von 1800 GB eingerichtet und darin eine Daten- und eine Archivpartition von je 500 GB. Nachdem ich die Daten- und Archivpartitionen mit Daten gefüllt waren, wollte ich die restlichen 800 GB der erweiterten Partition nutzen und eine große Film-Partition einrichten. Doch da teilte mir der Microsoft-Diskmanager lakonisch mit, es sei „ein Fehler aufgetreten“. Die erweiterte Partition war einfach verschwunden. Ein Fehler des Diskmanagers oder ein Kompatibilitätsproblem zwischen BIOS und Festplatte?

Außer einem größerem Zeitverlust war kein Schaden entstanden, ausgenommen an meiner Laune. Die alte Festplatte war ja noch da, und außerdem hatte ich ein Backup, das nur vier Tage alt war. Die Festplatte habe ich gegen ein 1000-GB-Modell eines anderen Herstellers getauscht und mit dem Kopieren noch einmal von vorn angefangen, diesmal funktionierte alles.

Und die Moral von der Geschichte?

Daten sind niemals völlig sicher, selbst simple Routinetätigkeiten können im Desaster enden.

2.3.3 Risiken durch Umwelt- und andere äußere Einflüsse

Überspannungen

- Blitzschlag in den Blitzableiter kann elektronische Geräte im Umkreis von 50 bis 100 Metern zerstören. Auch ein Blitzschlag in die Überlandleitung kann Schäden verursachen.
- Überspannungsspitzen durch Schaltvorgänge auf Hochspannungsleitungen,
- Überspannungen auf der Telefon-/DSL-Leitung,
- Elektrostatische Aufladungen.

Flüssigkeiten

- Die Waschmaschine in der Wohnung über Ihnen läuft aus.
- Ein Sturm oder eine Windhose beschädigen das Dach und ein Wolkenbruch folgt.
- Der Albtraum: Die Feuerwehr löscht einen Brand in der Etage über Ihnen.
- Wir wissen jetzt, dass „Jahrhundert-Hochwässer“ öfter als alle hundert Jahre auftreten.
- Wird der Computer, eine externe Festplatte, ein optisches oder magnetisches Laufwerk nach einem längeren Aufenthalt in der Kälte in einen warmen Raum getragen, kann sich Kondenswasser auf der Elektronikplatine bilden, was zu Kriechströmen und Kurzschlüssen führen kann.

Temperaturschwankungen

- Fast ausnahmslos bei allen Notebooks und bei vielen besonders kompakt gebauten PCs ist die Kühlung des Computers ungenügend.
- Eine erhöhte Betriebstemperatur verkürzt die Lebenserwartung der Festplatte. Die Überhitzung ist langfristig der größte Feind der Festplatte. Die meisten Desktop-Festplatten sind für eine Betriebsdauer von täglich maximal 10 bis 12 Stunden projektiert. Dauerbetrieb führt zu Überhitzung. Bei externen Festplatten und Notebook-Festplatten ist es noch kritischer. Fast alle werden schon nach sehr wenigen Stunden zu heiß.

2.3.4 Risiken durch Hardwareprobleme

Datenverluste durch physikalische Vorgänge

- Vibrationen im Betrieb oder Erschütterungen beim Transport sollten nicht unterschätzt werden.
- Das Erdmagnetfeld wirkt zwar schwach, aber ausdauernd auf die Magnetisierung ein.
- Die Bits auf einer Festplatte sind so winzig und liegen so dicht hintereinander in der Spur, dass sie sich allmählich gegenseitig ummagnetisieren. Es dürfte eine gute Idee sein, eine archivierte Festplatte jedes Jahr anzuschließen und die Daten durch Umkopieren aufzufrischen. Nebenbei werden dabei die Kondensatoren der Festplattenelektronik regeneriert.
- Das BIOS von Festplatten und optischen Laufwerken ist in ROMs gespeichert, die eine Haltbarkeit in der Größenordnung von zehn Jahren haben, bis die ersten Bits verloren gehen.
- Energiereiche kosmische Teilchen dringen gelegentlich bis zur Erdoberfläche vor. Hier können sie zu Einzelbit-Datenfehlern führen. In großer Höhe ist die Strahlung viel stärker, z. B. im Flugzeug in 12 km Höhe.
- Kontakte können durch Korrosion oder nachlassende Federkraft unsicher werden. Wenn ein Kontakt an der Festplatte für eine Millisekunde ausfällt, können tausende Bits verloren gehen.

Chemische Einflüsse

Ein andauerndes Problem ist der bei beschreibbaren optischen Scheiben verwendete Farbstoff. Er soll sich durch die Hitze des Brenn-Laserstrahls verfärben. Je weniger Hitze dafür gebraucht wird, desto höher kann die Brenngeschwindigkeit gesteigert werden. Doch je empfindlicher der Farbstoff, umso mehr verfärbt sich der Farbstoff bereits bei Zimmertemperatur, wenn auch sehr langsam. Allgemeingültige Aussagen sind schwierig, weil die Hersteller immer neue hitzeempfindliche Farbstoffverbindungen ausprobieren. Lassen Sie Ihre DVDs keinesfalls im Sonnenschein liegen! Die Stiftung Warentest hat festgestellt, dass die meisten einmalbeschreibbaren DVD-R Rohlinge eine miserable Lichtbeständigkeit haben, während die mehrfach beschreibbaren DVD-RW-Rohlinge höchst empfindlich gegen Wärme und Kälte sind.

Da sich jahreszeitliche Temperaturschwankungen bei der Lagerung kaum vermeiden lassen, sind RW-Rohlinge für eine lange Lagerung weniger geeignet. Medien im Dunkeln aufzubewahren ist kein Problem, deshalb erreicht man mit einmal-beschreibbaren Medien die längere Haltbarkeit.

Steck- und Lötverbindungen

Wo sich Metalle lange Zeit berühren, beginnen Oberflächenatome zu diffundieren. Vermutlich kennen Sie das Problem: Sie ziehen eine Schraube mit mäßiger Kraft an, doch nach ein paar Monaten oder Jahren sitzt sie fest wie angeschweißt. Im Computer stört es kaum, wenn die Schrauben fest sitzen. Es stört ein anderes Phänomen: Wo sich unterschiedliche Metalle berühren (z. B. Kontakte aus Gold und Silber), bilden sich sogenannte „intermetallische Phasen“, welche den Übergangswiderstand vergrößern.

Elektrochemische Korrosion

Steckt man eine Zink- und eine Kohleelektrode in eine leitfähige Lösung, ergibt das eine Batterie. Das klappt nicht nur mit Zink und Kohle, sondern zwischen beliebigen Metallen, zum Beispiel zwischen Kupfer, Silber, Gold und Lötzinn. Auch an Schraub- und Steckkontakten können zwei oder drei verschiedene Metalle aufeinandertreffen. Wo sich z. B. Silber und Gold berühren, entsteht eine Spannung von 0,6 Volt. Zwischen Kupfer und Zinn sind es 0,21 Volt. Zwischen einer Kupfermünze und einem Nagel, in eine Mandarine gesteckt, sind es 0,95 Volt. Sobald die Feuchtigkeit der Luft dazukommt, bildet sich ein galvanisches Element. Der Strom beginnt zu fließen, die Korrosion ist unabwendbar.

Thermisch beanspruchte Lötverbindungen

Alle Bauteile dehnen sich bei Erwärmung aus, je nach Material unterschiedlich: Kupfer 16, Aluminium 23, Zink 36, Polyethylen 100 bis 250, Porzellan 3 (Angaben in Millionstel der Länge pro °C). Nach dem Einschalten erwärmt sich der PC von 20 °C auf stellenweise bis 70 °C, die Spannungsregler im Netzteil und auf der Hauptplatine werden noch heißer. Die elektronischen Bauteile sind auf Leiterplatinen aufgelötet. Das Material der Leiterplatten (Polyethylen) dehnt sich bei Erwärmung etwa zehnmal stärker aus als das Kupfer der aufgeklebten Leiterzüge, Mikrorisse können die Folge sein.

Leider gilt seit 2005 in Europa die RoHS-Verordnung, welche die Verwendung von Blei zum Löten verbietet. Blei ist giftig. Es gibt zahlreiche alternative Lötlegierungen, doch keine reicht qualitativ an Bleilot heran. Die meisten bleifreien Lote sind schwierig zu verarbeiten und haben eine schlechte Langzeitstabilität. Ausnahme: Gold-Zinn-Lot ist langzeitstabil, hat aber einen zu hohen Schmelzpunkt, abgesehen vom Preis.

Wir müssen also langfristig mit anfälliger werdenden Lötstellen rechnen. Deshalb gibt es im Gesetz eine Ausnahmeregelung für sicherheitsrelevante Anwendungen (medizinische Geräte, Überwachungs- und Kontrollinstrumente, Autoelektronik und Militär): Hier darf weiterhin Bleilot verwendet werden. Heimelektronische Geräte mit langer Lebensdauer werden seltener werden. Die Hersteller wird es freuen, dass der Umsatz steigt.

Damit hatte niemand gerechnet

„Cirrus Logics“ lieferte Festplattencontroller an Fujitsu. Um halogenfrei zu produzieren, änderte Cirrus im Jahr 2002 die Rezeptur des Flammschutzmittels im Chipgehäuse, ohne Fujitsu zu informieren. Durch die Hitze unter der Festplatte bildete sich Phosphorsäure und zerfraß die Leiterplatte.

Fujitsu musste 4,9 Millionen Festplatten zurückrufen. Weil der Rückruf nicht schnell genug erfolgte, wurde Fujitsu von einigen Anwendern verklagt und musste jedem Kläger 1200 Dollar für die Datenrettung zahlen. Fujitsu wiederum verklagte den Zulieferer erfolgreich auf 40 Millionen Dollar Schadensersatz. Mehr dazu unter `http://www.theregister.co.uk/2002/11/05/fujitsu_admits_4_9_million/` (englisch).

Das ist nur **ein** Beispiel für die hochkomplexen Zusammenhänge in der Hochtechnologie. Jede scheinbar kleine Änderung in der Produktion kann entfernte Auswirkungen haben, an die einfach noch niemand gedacht hat.

2.3.5 Ungeahnte Risiken durch neueste Technologien

Notebooks werden in einem beträchtlichen Ausmaß verloren oder gestohlen. Einige dokumentierte Beispiele: Von 2005 bis 2007 wurden in den deutschen Bundesbehörden 326 von 53600 Laptops gestohlen. Dem Handelsministerium der USA gingen in fünf Jahren 1137 Notebooks verloren. In Großbritannien vermisste das Verteidigungsministerium 21 Notebooks im Jahr 2005 und das Innenministerium 19 Stück.

Um einen Konkurrenten auszuspionieren, braucht man nicht mehr in die Firma einzubrechen – es ist viel weniger riskant, einem der Ingenieure nachts das Notebook aus der Wohnung zu stehlen oder es ihm auf dem Parkplatz zu entwenden. Wenn vertrauliche Forschungs- und Finanzunterlagen in die Hände der Konkurrenz gelangen, kann der Schaden gewaltig sein. Deshalb verschlüsseln einige der neuesten Notebook-Festplatten sämtliche Daten beim Schreiben und Lesen automatisch. Sofort nach dem Einschalten des Notebooks muss der Schlüssel eingegeben werden. Wer den Schlüssel nicht kennt, kommt nicht an die Daten heran. Theoretisch jedenfalls.

Allerdings verwenden die meisten Benutzer viel zu simple Passwörter, die von Profis in wenigen Minuten oder Stunden zu „knacken“ sind. Die Industrie hat sich auch dagegen etwas einfallen lassen: Der Schlüssel wird bei einigen der neuesten Notebook-Festplatten automatisch gelöscht, wenn der Schlüssel mehrmals nacheinander falsch eingegeben wird. Wenn das Notebook in falsche Hände fällt oder der neugierige Sohn einige Passwörter durchprobiert, begeht die Festplatte vollautomatisch „Selbstmord“ und der komplette Inhalt der Festplatte ist weg – unwiderruflich, für immer.

2.4 RISIKO-MINIMIERUNG

Viele Risiken lassen sich durch Vorsicht und Umsicht verringern. Auf den folgenden Seiten geht es um weitere Möglichkeiten, Datenverluste zu vermeiden.

2.4.1 Stromversorgung

Schutz vor Spannungsschwankungen

Die Energieversorger müssen manchmal Umschaltungen vornehmen, beispielsweise um Überlandleitungen für Wartungsarbeiten stromlos zu schalten. Die meisten Umschaltungen erfolgen nachts. Jeder Schaltvorgang verursacht eine kurze Spannungsschwankung in den Leitungen. Diese Schwankung dauert meist weniger als eine Viertelsekunde und wird von der Energie ausgeglichen, die in den Pufferkondensatoren des PC-Netzteils gespeichert ist. Das Computernetzteil sollte damit problemlos klarkommen. Wenn der Strom aber eine Sekunde oder noch länger ausfällt, geht der PC aus und nicht gespeicherte Daten sind verloren.

Gefährlich ist es ebenfalls, wenn Ihr Wohngebiet von einem großräumigen, länger andauernden Stromausfall betroffen ist. In dem Moment, wenn der Strom wiederkommt, ist der Strombedarf extrem hoch. Beispielsweise laufen sämtliche Kühlschrankmotoren gleichzeitig an. Dieser Motortyp braucht im Anlaufmoment einen vielfach größeren Strom als im Dauerbetrieb. So kommt es zu mehreren Stromstößen, sogenannten „Einschwingvorgängen“, die kurzzeitig mehr als 1000 Volt erreichen können. Dadurch können der PC und andere elektronische Geräte beschädigt werden.

Auch eine durchgebrannte Schmelzsicherung kann zu Problemen führen. Beim Einschrauben einer neuen Sicherung gibt es praktisch immer mehrere Stromstöße (beobachten Sie einmal, wie oft dabei das Licht flackert).

Gewöhnen Sie sich an, am Arbeitsende PC, Bildschirm und Lautsprecher mittels schaltbarer Steckdosenleiste abzuschalten. Sie sparen etwa 30 € pro Jahr und außerdem schützen Sie Ihren PC vor nächtlichen Überspannungen. Wenn Sie eine Steckdosenleiste mit integriertem Überspannungsschutz verwenden, ist Ihr PC auch am Tage weitgehend vor Überspannungen geschützt.

Schutz vor Blitzschlägen

Durch Blitzschläge entstehen weitaus höhere Störspannungen, die eine abgeschaltete Steckdosenleiste überspringen. Nicht nur direkte Treffer in den Blitzableiter Ihres Hauses sind gefährlich, auch Blitzeinschläge in der Nachbarschaft können in Ihren Strom- und Telefonleitungen hohe Störspannungen erzeugen. Deshalb ist es eine gute Idee, bevor Sie in Urlaub fahren oder wenn ein schweres Gewitter im Anzug ist, den PC (und weitere elektronische Geräte) vom Stromnetz zu trennen (gemeint ist: Stecker herausziehen!). Die Fernsehantenne, das Telefon und den DSL-Anschluss können Sie gleich mit herausziehen.

Schutz vor Spannungsausfällen

Für besonders wichtige PC kann eine Notstromversorgung sinnvoll sein, vor allem in Gegenden mit häufigen Stromschwankungen und -unterbrechungen. Eine USV (**U**nterbrechungsfreie **S**trom-**V**ersorgung, englisch **U**ninterruptible **P**ower **S**upply (UPS)), erzeugt einige Minuten lang eine Ersatz-Netzspannung aus der gespeicherten Energie eines Akkus. Für kommerziell genutzte Server wäre es unverzeihlicher Leichtsinn, auf eine USV zu verzichten. Rechenzentren haben zusätzlich Notstrom-Dieselaggregate für längere Stromausfälle .

Die einfacheren „Offline-USV“ beginnen erst dann Strom zu erzeugen, wenn die Netzspannung ausfällt. Dadurch kommt es zu einer kurzen Umschaltpause von etwa 5 Millisekunden, die kein Problem für den PC darstellt. Solche Geräte kosten weniger als 100 Euro und sind für die meisten Anwendungsfälle völlig ausreichend.

Die „Online-USV“ sind die Königsklasse. Die angeschlossenen PC sind nicht mit der Netzspannung verbunden, sie werden ausschließlich mit dem Strom versorgt, der aus der Akkuladung erzeugt wird. Mit dem Netzstrom, solange er verfügbar ist, wird der Akku nachgeladen. Von Schwankungen der Netzspannung oder der Frequenz bekommt der PC nichts zu spüren. Allerdings sind diese Geräte teuer. Bei der ununterbrochenen Umwandlung von 230 Volt in die Akku-Spannung und wieder zurück in 230 Volt entsteht viel Abwärme, ohne einen deutlich hörbaren Lüfter kommt eine solche USV nicht aus.

2.4.2 RAID

Der Begriff RAID steht für eine Technologie, bei der die Daten auf mehrere Festplatten verteilt werden. Die Festplatten werden zu einer logischen Einheit zusammengeschaltet. Das bedeutet: Für das Betriebssystem erscheint der RAID-Verbund wie eine einzige Festplatte.

Je nachdem, wie die Festplatten zusammengeschaltet sind, kann dreierlei passieren:

- Weil sich die Festplattenzugriffe auf mehrere Festplatten verteilen, wird das System schneller als eine einzelne Platte.
- Wenn die Daten auf geeignete Weise dupliziert werden, kann bei Ausfall einer der Festplatten deren Inhalt aus dem Inhalt der anderen Platten automatisch rekonstruiert werden. So tritt kein Datenverlust ein, mehr noch: Die Arbeit geht unterbrechungsfrei weiter. Bei Gelegenheit wird die defekte Platte ausgewechselt.
- Eine Kombination beider Effekte ist möglich.

Die verschiedenen Verfahren werden mit Ziffern bezeichnet. Die gebräuchlichsten Verfahren sind RAID-0, 1, 5 sowie RAID-10. Die Verfahren RAID-2 und RAID-3 sind veraltet und werden nicht mehr verwendet. Die Verfahren mit Nummern oberhalb der 10 sind exzessiv teuer und für Normalanwender uninteressant.

RAID-0

Bei diesem auch „Data Striping" genannten Verfahren werden zwei oder mehr Festplatten so zusammengeschaltet, dass aufeinanderfolgende Datenblöcke reihum auf alle Festplatten verteilt werden. Die resultierende Geschwindigkeit steigt. Je mehr Festplatten zusammengeschaltet werden, desto höher die Geschwindigkeit. Besonders bei Videoschnittsystemen ist der Geschwindigkeitsgewinn beträchtlich.

Allerdings hat RAID-0 einen gefährlichen Nachteil: Je mehr Festplatten benutzt werden, desto höher wird die Ausfallwahrscheinlichkeit. Wenn eine der Festplatten ausfällt, sind alle Daten verloren, auch die auf den restlichen, intakten Festplatten. Die Ausfallwahrscheinlichkeit steigt ungefähr proportional zur Anzahl der Festplatten.

RAID-1

Die technologisch einfachste RAID-Lösung ist „RAID-1", die auch unter den Bezeichnungen „Spiegelung", „Drive Mirroring" oder „Drive Duplexing" bekannt ist. Jede mit Daten gefüllte Festplatte wird um eine weitere, baugleiche Festplatte ergänzt, die mit dem Duplikat der Daten gefüllt wird. Wenn Sie z. B. zwei Festplatten mit Daten haben, würden Sie zwei zusätzliche Festplatten für deren Spiegelung brauchen. Das ist teuer.

Für das Duplizieren der Daten gibt es Hardware- und Softwarelösungen. Viele moderne Hauptplatinen haben einen integrierten RAID-Controller, der das Duplizieren der Daten übernehmen kann. Das Schreiben auf zwei Platten dauert etwa ebenso lange wie das Schreiben auf eine einzelne Platte. Beim Lesen kann RAID-1 einen leichten Geschwindigkeitsvorteil haben, weil der Controller sich aussuchen kann, auf welcher der beiden Festplatten sich die Daten näher an der aktuellen Position des Lese-/Schreibkopfes befinden.

RAID-1 als Softwarelösung wird nur von Server-Betriebssystemen beherrscht. Das Betriebssystem schreibt jeden Datenblock nacheinander auf beide Festplatten. Dadurch tritt beim Schreiben ein kleiner Verlust an Geschwindigkeit ein. Beim Lesen gibt es ebenso wie bei der Hardwarelösung einen Geschwindigkeitsgewinn, weil sich die Lesezugriffe auf beide Festplatten verteilen lassen.

RAID-5

Bei „RAID-5" wird zu zwei oder einer beliebig größeren Anzahl von Festplatten nur eine einzige zusätzliche Paritäts-Festplatte hinzugefügt. Das Verfahren ist so ähnlich wie das Hinzufügen eines Paritätsbits zu jedem Byte. Die Paritätsinformation wird vom Controller gebildet. Die Paritätsinformationen werden auf alle Festplatten des Verbandes gleichmäßig verteilt. Bei Ausfall einer beliebigen Festplatte rekonstruiert der Controller die Daten aus dem Inhalt der verbliebenen Festplatten. Dadurch gehen keine Daten verloren, mehr noch: Der PC kann ohne Unterbrechung und ohne Datenverlust weiterarbeiten.

RAID-5 ist ein hervorragender Kompromiss zwischen Kosten, Leistung und Sicherheit. Die Geschwindigkeit wächst wie bei RAID-0 mit der Anzahl der Festplatten. Das hohe Risiko eines Festplattenausfalls von RAID-0 wird durch eine einzige zusätzliche Festplatte kompensiert.

RAID-6

Für noch höhere Ansprüche gibt es „RAID-6". Dabei werden zwei Reservefestplatten verwendet, so dass selbst bei Ausfall beliebiger zweier Festplatten weitergearbeitet werden kann. Allerdings ist das Berechnen der Paritätsinformation recht aufwändig, worunter die Geschwindigkeit leidet.

RAID-10

Bei RAID-10 werden RAID-1 und RAID-0 kombiniert. Es wird eine gerade Anzahl von gleich großen Festplatten benötigt. Die Festplatten werden paarweise gespiegelt. Dann werden die RAID-1-Paare wie bei RAID-0 zu einem übergeordneten Verbund zusammengeschaltet. Der Hardware-Aufwand ist hoch, aber

die Geschwindigkeit auch. RAID-10 verkraftet sogar den Ausfall mehrerer Festplatten ohne Datenverlust, solange es nicht beide Platten eines Pärchens trifft.

Sonstige RAID-Lösungen

Es gibt zahlreiche weitere RAID-Lösungen, die sich in Ausfallsicherheit, Kosten und Geschwindigkeit unterscheiden. RAID10 funktioniert weiter, auch wenn zwei Festplatten ausgefallen sind. Bei RAID-51 dürfen von acht Festplatten beliebige drei ausfallen, ohne dass Daten verloren gehen. Beeindruckend!

Vor- und Nachteile aller RAID-Lösungen

Nachteile

- Außer bei RAID-1 in Servern braucht man einen speziellen Festplattencontroller, der sehr teuer sein kann. Deshalb sind RAID-5-Lösungen (und höher) vor allen in Servern zu finden. Es gibt aber auf vielen hochwertigen Hauptplatinen integrierte RAID-5-Controller.

Vorteile

- Weil sich die Leseanforderungen auf mehrere Festplatten verteilen, steigt der Datendurchsatz des Systems deutlich an. Je mehr Festplatten, desto schneller.
- An einfachere Controller können bis zu 15 Festplatten angeschlossen werden, teure Modelle können 45 Platten ansteuern. Da man mehrere dieser Controllerplatinen in einen Server stecken kann, ist die Zahl der anschließbaren Festplatten sehr hoch.
- Wenn der Speicherplatz knapp wird, ergänzt man den RAID-Verband um eine oder mehrere zusätzliche Festplatten. Viele Controller können die vorhandenen Daten bei laufendem Betrieb umverteilen. Einige Stunden später steht die größere Kapazität zur Verfügung. Aber Vorsicht! Die Menüs der Controller sind in Englisch und darüber hinaus oft so unübersichtlich, dass dieses „einfache“ Hinzufügen hochgradig riskant sein kann. Ich empfehle dringend, vorher eine vollständige Datensicherung durchzuführen oder – falls das möglich ist – ein Image zu erstellen!

Probleme

Ein RAID-System schützt nur vor dem Ausfall einer Festplatte und der damit zusammenhängenden Betriebsunterbrechung. Die meisten Daten gehen durch andere Ursachen verloren, weniger als 20 % aller Datenverluste werden durch einen Festplattenausfall verschuldet. Insoweit kann ein RAID-System kein Ersatz für eine Datensicherung sein. Eine regelmäßige Sicherung auf ein geeignetes Medium ist unbedingt notwendig!

Der erste von mir verkaufte RAID-Controller kostete 4500 DM. Zehn Festplatten waren angeschlossen, das System war atemberaubend schnell. Ich werde nie den Tag vergessen, an dem der Lüfter des RAID-Controllers ausfiel – ohne Warnsignal. Der Controller hatte zwar einen eigenen Lautsprecher, um Fehler an den Festplatten lautstark zu melden, aber der Controller überwachte weder seinen eigenen Lüfter noch die Temperatur des eigenen Prozessors. Jedenfalls fiel der Lüfter aus, die CPU des Controllers wurde zu heiß und stürzte ab. Die Verwaltungstabellen der Festplatten wurden beschädigt. Alle Daten waren rettungslos verloren!

Doch zum Glück hatte ich den Kunden überzeugen können, in jeder Nacht eine Datensicherung auf Band durchzuführen. Ohne diese Bandsicherung der letzten Nacht hätte ich mich wohl beeilen müssen, mein Testament zu schreiben, bevor der Inhaber der betroffenen Firma erschienen wäre, um erst mich und dann sich selbst zu erschießen.

Wenn eine der Festplatten eines RAID-Verbandes ausfällt, muss sie schnellstens durch eine neue ersetzt werden. In die hochwertigsten Systeme sind eine oder mehrere Reservefestplatten eingebaut, die als Hot Spare oder Hot Fix bezeichnet werden. Die Reserveplatte wird automatisch eingeschaltet und an Stelle der defekten Festplatte integriert. Dadurch wird die Redundanz auch ohne Eingreifen eines Administrators automatisch wiederhergestellt.

Bei einfacheren Controllern muss man den PC herunterfahren, um die Festplatte zu wechseln. Manchmal ist diese Betriebsunterbrechung nicht akzeptabel, z. B. bei Servern. Wenn die Festplatten in speziellen Einschüben stecken und der Controller „Hot-Plugging“ (das heiße Einstecken) unterstützt, können die Festplatten im laufenden Betrieb ausgetauscht werden. Dazu müssen die Festplatten in speziellen Einschüben stecken. Der Start der Rekonfiguration muss vom Administrator ausgelöst werden.

In großen Rechenzentren wird das „Hot Swapping“ (der heiße Austausch) bevorzugt: Die Platte wird im laufenden Betrieb gewechselt, und es wird keine Fachkraft benötigt, um defekte Festplatten auszutauschen, denn der Controller integriert die neue Festplatte automatisch, ohne Eingreifen eines Administrators.

Beim Austausch einer defekten Festplatte gibt es eine wenig bekannte Gefahr. Alle Platten des Verbundes sind vermutlich im Abstand weniger Minuten vom Fließband gelaufen. Sie sind deshalb mechanisch äußerst ähnlich und haben etwa die gleiche Lebenserwartung. Während des Betriebes hatten sie immer die gleiche Belastung auszuhalten. Nach dem Ausfall der ersten Festplatte könnten die nächsten bald nachfolgen!

Die Festplatten eines RAID-Systems sind im Normalbetrieb relativ wenig beansprucht, denn die Lese- und Schreibanforderungen werden nahezu gleichmäßig auf alle Platten verteilt. Doch nach dem Einsetzen der Ersatzfestplatte ändert sich das: Der RAID-Controller wird stundenlang mit Höchstlast laufen, um die Daten umzustrukturieren und die neue Festplatte zu integrieren. Das kann durchaus 24 Stunden und länger dauern. Noch nie zuvor sind Ihre Festplatten derart beansprucht, derart heiß geworden! Das führt nicht selten zum Ausfall einer weiteren Festplatte, siehe vorherigen Hinweis. Besonders oft passieren solche Pannen bei Plattenspiegelungen von SATA-Festplatten in Heimcomputern. Die hier üblicherweise verwendeten Festplatten sind nicht für derartige lang andauernde Belastungen konzipiert. Deshalb sollten Sie zuerst eine komplette Sicherung durchführen und erst danach die Festplatte auswechseln. Doch die Datensicherung ist ebenfalls eine – wenn auch wesentlich kleinere – hohe Belastung für die Festplatten und sollte in Etappen mit Abkühlpausen durchgeführt werden.

Die Platten eines RAID-Verbandes müssen in der Regel identische Größe haben. Andernfalls wird von jeder Festplatte nur so viel an Kapazität benutzt, wie die kleinste der Festplatten hat. Will man eine ausgefallene Festplatte ersetzen, darf die Kapazität der Ersatzfestplatte auch nicht um ein einziges Byte kleiner als die Kapazität der anderen sein. Wenn die neue Festplatte erheblich größer ist, kann der „Kapazitäts-Überschuss“ als gewöhnliche, nicht-redundante Partition genutzt werden.

Ein Ausfall des Controllers kann ein sehr ernstes Problem sein. Wenn man kein identisches Ersatzexemplar besorgen kann (Hardware und Firmware müssen übereinstimmen), können die ansonsten intakten Festplatten möglicherweise nicht mehr gelesen werden. Das kann bei No-Name-Controllern ein Problem sein, ebenso bei auf Hauptplatinen integrierten Controllern. Sicherheitsbewussten Anwendern muss man raten, vom Controller bzw. der Hauptplatine zwei Stück zu kaufen. Solange das Duplikat nicht benötigt wird, kann es in einem Arbeitsplatz-PC gute Dienste leisten. Andernfalls müssen Sie Ihr ganzes Vertrauen in die Datensicherung setzen.

2.4.3 Wo sollten die Datenträger gelagert werden?

Achten Sie darauf, dass einige der der Sicherungsmedien räumlich weit entfernt vom PC gelagert werden. Was nützt Ihnen eine Sicherung, wenn sie zusammen mit dem PC bei einem Diebstahl mitgenommen oder durch einen Brand, Löschwasser oder Hochwasser zerstört wird?

Private Daten können Sie auf eine DVD brennen und einem guten Freund oder Verwandten zur Aufbewahrung geben. Eine DVD im Keller zu lagern (luftdicht verpackt wegen der Feuchtigkeit), kann eine brauchbare Idee sein (wenn der Keller nicht überschwemmungsgefährdet ist und nicht zu oft von Dieben besucht wird). In beiden Fällen sollten Sie über eine Verschlüsselung nachdenken.

Mein Sohn schenkt mir und seinem Bruder alljährlich zu Weihnachten eine DVD mit den Familienfotos des letzten Jahres. Den restlichen Platz auf der DVD kann er für einen verschlüsselten Container mit seinen wichtigsten Daten nutzen. Ich sehe mir die Fotos gern an, und er hat auf diese Weise zwei Sicherungskopien auswärts gelagert.