Datenrettung

im Proseminar *"Speicher- und Dateisysteme"*

Bernd Themann

Inhaltsverzeichnis

1 Allgemeines zum Thema Datenrettung

1.1 Einführung

Bei der Datenrettung (engl.: Data Recovery) wird versucht gelöschte bzw. defekte Daten wiederherzustellen. Dies ist nötig wenn es auf konventionellem Weg nicht mehr möglich ist auf die Daten eines Speichermediums zuzugreifen. Für einen Datenverlust kann es die unterschiedlichsten Gründe geben, unter anderem menschliche Fehler, Malware oder mechanische Defekte.
Hardwareprobleme gehören dabei allerdings mit 59% zu der häufigsten Fehlerquelle, gefolgt von Anwendungsfehlern (26%) und Softwarefehlern (9%). Die restlichen 6% teilen sich jeweils Viren/Würmer, Naturkatastrophen und alle anderen nicht erfassten Fehlerquellen[4].
Man unterscheidet logische und physische Fehler. Erstere liegen immer dann vor, wenn die Hardware (Festplatte, USB-Stick, usw.) intakt ist, die Daten jedoch nicht mehr direkt ausgelesen werden können. Bei physischen Fehlern ist es genau umgekehrt, dort lässt sich die Hardware nicht mehr auslesen. Natürlich können auch Kombinationen aus beiden Fehlerarten auftreten.
Je nach Fehlerart unterscheidet sich das Vorgehen und der Aufwand bei der Datenwiederherstellung erheblich. Während bei logischen Fehlern oft Wiederherstellungstools weiterhelfen können, muss bei physischen Fehlern in den meisten Fällen auf professionelle Hilfe mit dementsprechendem Profiequipment zurück-gegriffen werden.
Es gibt eine große Anzahl von Firmen, die sich auf die Rettung von Daten spezialisiert haben. Zu den größten international tätigen Datenrettungsfirmen gehört unter anderem Convar, KUERT, CBL und Kroll Ontrack. Letztere bietet sogar eine patentierte “Remote Data Recovery” (RDR) an, bei der die Datenrettung vor Ort über das Internet vorgenommen wird [1]. Convar wirbt mit seinem “Real Time Online Information System”, über das der Kunde zu jeder Zeit den Fortschritt seiner Datenrettung online einsehen kann. Zudem legt die Firma besonderen Wert auf Sicherheit und erfüllt durch biometrische Zugangskontrollen und besonders gesicherte Safes die US Militärnormen für sensitive Daten. Das Serviceangebot der genannten Firmen unterscheidet sich ansonsten nur marginal von einander. Die Datenrettung einer Vielzahl von Speichermedien unabhängig von dem verwendeten Betriebssystem wird von allen angeboten.

1.2 Vorgehen bei logischen Fehlern

Unter diese Kategorie fallen alle Fehler, bei denen es aufgrund von Schäden in der logischen Struktur des Speichermediums für das Betriebssystems nicht mehr ohne weiteres möglich ist die Daten auszulesen. Damit das Betriebssystem die Daten zuordnen kann, werden diese im Dateisystem gespeichert. Das Dateisystem verwaltet neben Verzeichnissen mit Dateinamen und den Dateiinhalten noch weitere Dateiattribute. Zur Speicherung der Daten in dieser logischen Struktur benötigt es eine Vielzahl von Abläufen, die normalerweise automatisch ablaufen und nicht vom Benutzer beeinflussbar sind. Ist

[1] diese Wiederherstellungsoption kann nur bei logischen Fehlern angewendet werden

diese logische Struktur nun beschädigt, kann das System die Daten nicht wiederfinden. Aber auch bei einer unbeschädigten Struktur kann es sein, dass benötigte Daten nicht mehr abfragbar sind. Zum Beispiel in dem Fall, wenn der Benutzer unachtsam Dateien gelöscht hat. Normalerweise lassen sich diese Dateien bzw. Daten wiederherstellen, da das Betriebssystem lediglich die Zuordnung löscht und nicht die Daten selber. Ist der Master Boot Record (MBR) beschädigt, kann der Computer gar nicht mehr gestartet werden, da die Partitionierung der Festplatte nicht mehr erkannt wird. Die Daten auf der Partition selber sind davon jedoch unberührt.

Um bei diesen Fehlern die Daten wieder lesbar zu machen, muss also die Zuordnungen und die logische Struktur wiederhergestellt werden. Der erste Schritt dabei ist, die Daten auf dem Speichermedium zu lokalisieren und zu identifizieren. Die Schwierigkeit hier liegt bei der Vielzahl an verwendeten Dateisystemen und der damit einhergehenden unterschiedlichen Strukturierung der Daten. Als wichtigste Dateisysteme seien Fat/Fat32 (Speicherkarten,...), NTFS (Windows), ext (Linux) und HFS (Max OS X) genannt. Besondere Probleme machen den Rettungslaboren RAID-Systeme und verschlüsselte Speicher, da die Hersteller dieser oft die Algorithmen und logische Struktur der Daten geheim halten.
Konnte die zu wiederherstellenden Dateien im ersten Schritt gefunden und identifiziert werden, muss nun die Referenz im Dateisystem neu erstellt werden[2]. Dann sollte es wieder möglich sein auf die Daten zuzugreifen. Mit spezieller Software lassen sich Fehler dieser Kategorie mit hoher Wahrscheinlichkeit beseitigen. Die Programme dazu sind zum Teil im Internet frei verfügbar, zum Teil lassen sich diese auch direkt von den Datenrettungslaboren entgeltlich erwerben [3]. Dadurch haben versierte Benutzer gute Chancen derartige Fehler auch selber zu beheben.

1.3 Vorgehen bei physischen Fehlern

Bei physischen Fehlern handelt es sich um Defekte an der Hardware. Dazu zählt zum Beispiel ein durchgebrochener USB-Stick, eine zerkratzte CD oder eine Festplatte mit defektem Controller. Es kann sich hierbei um mechanische (vor allem bei Festplatten) oder elektronische Fehler handeln. Manchmal lassen sich diese Fehler selber beheben, oft aber ist dafür teures Spezialequipment notwendig. Gerade bei Festplatten ist die Behandlung des Mediums im Reinraum unabdingbar. Fehlerhafte Behandlung durch Laien führt oft zur Verschlechterung des Zustandes und zur dauerhaften Vernichtung der Daten.

1.4 Kosten-Nutzen Vergleich

Während bei privaten Nutzern deren Daten eher einen ideellen Wert haben, lässt sich der Wert hingegen im Geschäftsumfeld relativ präzise bestimmen. Gehen zum Beispiel durch einen Crash Kundendaten verloren, kann man mit Hilfe des durchschnittlichen Umsatzes pro Kunde recht genau abschätzen, wie hoch sich der Schaden, der durch

[2] bei defektem MBR muss dieser dementsprechend wiederhergestellt werden
[3] z.B.: Ontrack EasyRecovery DataRecovery

den Crash verursacht wurde, belaufen wird. Aber auch andere Faktoren wie die Zeit und Imageschäden spielen einen entscheidende Rolle. Eine von dem Ponemon Institute durchgeführte Studie ergab, dass sich der Schaden pro verlorenen Kundensatz im Schnitt auf 62$ beziffern lässt. Zählt man jedoch Folgekosten hinzu, beträgt der Schaden rund 177$[5]. Dies hängt damit zusammen, dass nach einem Datenverlust eine signifikant erhöhte Kundenfluktuation, sowie markant rückläufige Umsätze pro Kunde gemessen wurden. Die daraus resultierenden Einnahmeverluste führten in der Regel auch zu höheren Ausgaben für Marketing und Werbung. Betroffene Unternehmen mussten ihren Ruf in der Öffentlichkeit wiederherstellen um so wieder ihre Kunden zurückzugewinnen.
Allerdings sollte erwähnt werden, dass die meisten Firma über den Wert ihrer Daten informiert sind und dementsprechend Absicherungen treffen und redundant abspeichern. Das erklärt auch, wieso laut der der Studie die meisten Schäden durch verlorene oder geklaute mobile Endgeräte entstehen. Bei diesen ist es schwerer redundant zu speichern und es müsste auf Onlinebackups zurückgegriffen werden. Dies ist auf Grund von beschränkten Bandbreiten und aus Sicherheitsgründen nicht immer überall möglich.

2 Data Recovery einzelner Speichermedien

2.1 Festplatten

Mit einem Anteil von zirka 80 Prozent aller Datenrettungsfälle zählen Festplatten zu den häufigsten wiederherzustellenden Medien. Dies mag zum einen an der hohen Speicherkapazität und der großen Verbreitung dieses Mediums liegen, aber auch an der hohen Anzahl an Fehlerquellen. Die gesamte Controller-Elektronik, der Elektromotor, die besonders empfindlichen Leseköpfe und die Platter [4] sind mögliche Fehlerquellen. Defekte können etwa durch mechanische Einflüsse wie Stürze - besonders häufig bei Notebooks - oder durch Überspannung hervorgerufen werden. Letzteres gehört zu den häufigsten Ausfallursachen bei Desktop-Festplatten. Defekte oder qualitativ minderwertige Netzteile, die Spannungsspitzen nicht filtern bzw. selber erzeugen können Schäden an der Controllerelektronik hervorrufen.

2.1.1 Überblick über die Ursachen

Je nachdem welches der unzähligen Bauteile beschädigt ist, ergibt sich eine andere Wiederherstellungsstrategie. Um den Umfang nicht zu sprengen können im Folgenden nur die wichtigsten Fälle beschrieben werden, denn selbst mit Kaffee überschüttete Magnetscheiben und aufgebohrte Festplatten wurden in den Datenlaboren schon abgegeben. Es gibt auf den Kern reduziert 3 wichtige Einflussgrößen und Störungen. Diese haben unterschiedlichste Auswirkungen:
mechanische Einflüsse
Schläge und Stöße während des Betriebes einer Festplatte können nicht nur schnell

[4] Platter sind die Scheiben auf denen die eigentlichen Daten gespeichert werden

zu einem "Headcrashführen, sondern auch andere Teile wie die Elektronik im Inneren der Festplatte beschädigen. Besonders häufig sind von dieser Fehlerquelle mobile Endgeräte betroffen. Um die Auswirkungen zu reduzieren integrieren einige Hersteller Beschleunigungssensoren, die bei Lageänderungen den Schreibkopf in eine Parkposition fahren - gerade um einen Head-Crash zu vermeiden. Leider zeigt die Erfahrung, dass auch diese Schutzmaßnahme in der Realität eher ineffektiv sind.

Überhitzung
Die Überhitzung der Festplatte kann viele Defekte hervorrufen. Bei extremer Hitze (Brand oder ähnlichem) wird die Curie-Temperatur, jene Temperaturgrenze, bei denen die ferromagnetischen Eigenschaften verloren gehen, überschritten. Dies führt unweigerlich zum totalen Verlust aller Daten. Aber auch schon deutlich niedrigere Temperaturen können die Lebensdauer der Festplatte erheblich reduzieren. Normalerweise wird für Desktop-Festplatten eine Temperatur von 0 - 65 Grad[5] Celsius empfohlen. Trotzdem erhöht sich die Ausfallwahrscheinlichkeit mit höheren Temperaturen auch innerhalb dieser Spanne enorm. Auf der Platte befindet sich eine dünne Schutzschicht, die die Schäden bei einer Kollisionen (leichter Art) mit dem Schreibkopf minimieren sollen. Mit steigender Temperatur verändert diese ihre Konsistenz und verliert ihre Wirkung. Aber auch die Flüssiglagerung moderner Festplatten ist von einem Temperaturanstieg betroffen und so kann es passieren, dass die Platten ins Schlingern geraten. Ein Head-Crash ist in beiden Fällen sehr wahrscheinlich.

Überspannung
Überspannungen sind, wie vorher bereits beschrieben, die häufigste Ausfallursache im Privatanwender Bereich. Grund hierfür sind häufig Netzteile mit mangelnder Qualität. Diese sind nicht in der Lage Spannungsspitzen aus dem Stromnetz (etwa durch einen Blitzschlag ausgelöst) auszugleichen bzw. erzeugen selber welche. Ein solche Spannungsspitze im Stromnetz des Computers gefährdet die gesamte Elektronik, auch die der Festplatte. Die Folge ist ein Defekt an der Festplatten Elektronik, wodurch ein Zugriff auf die Daten nicht mehr möglich ist. Zum Glück ist die physische Speicherung der Daten in den meisten Fällen nicht betroffen.

2.1.2 Wiederherstellung der Daten

Defekter Controller
der Controller ist für die Steuerung der gesamten Festplatte zuständig. Ein Defekt dieses ist trotzdem in den meisten Fällen noch relativ unproblematisch zu beheben. Die Datenrettungslabore haben für diesen Fall eine große Sammlung unterschiedlicher Controller parat und tauschen diesen dann aus. Danach müsste ein ordnungsgemäßer Betrieb der Festplatte wieder möglich sein.

Defekt der Platter / Leseköpfe

[5] Quelle sind Datenblätter einzelner Festplatten von Western Digital, Seagate und Samsung

Der "Head-Crash"gehört zu den verheerendsten Defekten. Dabei berührt der Schreibkopf die empfindlichen Magnetscheiben. Normalerweise schwebt dieser getrennt und stabilisiert durch eine Luftschicht zwischen den einzelnen Platter. Die zusätzliche Schutzschicht die sich auf den Magnetscheiben befindet wird von diesem durchdrungen und die darunterliegende Datenschicht wird abgetragen. In diesem Bereich sind die Daten mit sehr hohen Wahrscheinlichkeit nicht mehr rekonstruierbar und die Magnetscheiben müssen in einem Reinraum extrahiert werden. Auch bei einer sehr kurzen Berührung, etwa durch einen Schlag, sind direkte Schäden und Folgeschäden zu erwarten. Bei Desktop-Festplatten drehen sich die Magnetscheiben üblicherweise mit 7200 U/min. Dabei "fliegt" der Schreibkopf mit rund 80 km/h[6] über die Platte. Bei einem Kontakt beider werden Partikel von der Magnetscheibe abgeschliffen welche sich wiederum zwischen Schreibkopf und Magnetscheibe setzen können und somit Folgeschäden verursachen. Aus diesem Grund ist der weitere Betrieb einer Festplatte mit Verdacht auf einen Headcrash (Schleifgeräusch das man von außen hören kann) aus Sicht der Datenwiederherstellung grob fahrlässig.
Bei besonders starken Defekten an den Magnetscheiben werden diese im Datenrettungslabor in einem Speziallabor (weitere Informationen siehe 3.3) extrahiert und speziell behandelt. Da die meisten Datenrettungslabor ihr genaues Vorgehen als Betriebsgeheimnis hüten, ist darüber dementsprechend wenig bekannt. Bekannt ist aber, dass die Platten als erstes in einer Spezialreinigung gereinigt werden. Diese soll Verschmutzungen entfernen und das weitere Auslesen der Daten erleichtern. Mit einer speziellen Maschine, oft eine Eigenentwicklung, können dann die Bereiche auf den einzelnen Magnetscheibe ausgelesen werden, die nicht zu stark beschädigt sind. Dabei wird mit einem Lesekopf jedes einzelne Bit gelesen und so versucht die Daten wiederherzustellen.
Bei leichteren Beschädigungen wird versucht den Actuatorarm mit den jeweiligen Leseköpfen durch einen baugleichen auszutauschen, um dann das Laufwerk wieder in Betrieb nehmen zu können.

2.2 Optische Medien (CD, DVD, BluRay)

Vom schematischen Aufbau unterscheiden sich die heutzutage gebräuchlichen optischen Medien kaum bis gar nicht. Lediglich die Weiterentwicklung der Laser ermöglichte es im Laufe der Zeit immer mehr Daten auf gleichen Raum zu schreiben und somit die Datendichte zu reduzieren. Dazu musste allerdings die Polycarbonat-Schicht auch immer weiter reduziert werden. Je dichter die Bits jedoch "nebeneinander" liegen, umso schwerer ist es auch diese Auszulesen und umso leichter können Kratzer oder Verunreinigungen zu Lesefehlern führen.

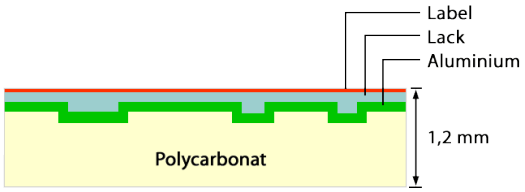

Abbildung 1: Schematischer Aufbau einer CD

Kratzer im Polycarbonat brechen den Laser und führen somit dazu, dass dieser die Oberfläche der Datenschicht nicht mehr korrekt erfassen kann. Da derartige Lesefehler

[6] Außen gemessen bei einem Durchmesser von 6 cm: $2 * \pi * 3cm * 7200U/min \approx 80km/h$

sehr oft Auftreten wird versucht durch Fehlerkorrektur das Medium trotzdem wieder lesbar zu machen. Die beiden wichtigsten Fehlerkorrekturen sind Paritätsbits und Interleaving.
Paritätsbits sind Bits die zu den eigentlichen Daten hinzugefügt werden um eine Redundanz zu erzeugen. In ihnen werden Informationen zu einzelnen Datenbereichen gespeichert. Möglich wäre zum Beispiel zu speichern ob die Quersumme eines Bytes gerade oder ungerade ist. Stimmt diese Information dann nicht mit den gerade gelesenem Byte überein muss ein Lesefehler aufgetreten sein. Je größer diese Redundanz ist, umso besser lassen sich die Lesefehler erkennen und beheben. Sind jedoch ganze Bereiche nicht mehr lesbar hilft diese Art der Fehlerkorrektur nicht weiter.
Um auch dieses Problem zu umgehen führte man das *Interleaving* ein, welches als Hauptziel hat, dass zusammengehörende Daten nicht direkt hintereinander auf das Medium gespeichert werden. So werden bei kleinen Kratzern die Lesefehler auf mehrere Datenpakete verteilt. Diese können dann bestenfalls wiederum durch die Paritätsbits ausgeglichen werden.[1]

2.3 Flashspeicher-Medien

Die Verbreitung von Flashspeichern nimmt stetig zu und es ist zu erwarten, dass diese in naher Zukunft der Festplatten den Rang ablaufen werden. Dementsprechend wird die große Rolle der Festplatten bei der Datenwiederherstellung mit der Zeit sinken.
Flashmedien haben den großen Vorteil, dass diese deutlich unempfindlicher gegen mechanische Einflüssen sind und die Daten in diesen nicht magnetisch gespeichert werden. Die Hersteller geben daher eine Speicherung der Daten von 10 Jahren an. Dies kann bei Festplatten nicht garantiert werden, da die magnetischen Informationen durch natürliche Effekte schwinden.
Der größte Unterschied zwischen den momentan zum Einsatz kommenden verschiedenen Flashspeicher-Typen ist der Aufbau der Zellarchitektur, welche maßgeblich für das Speichervolumen, Tempo, Preis und Lebensdauer des Speichers ist. Man unterscheidet zwischen der *SLC (Single Level Cell)*, bei der jede Zelle nur mit einem Bit beschrieben wird, und der *MLC (Multi Level Cell)*, bei der mehrere Bits in eine Zelle geschrieben werden. Dementsprechend hat erstere ein höheres Preis/Speicherplatz Verhältnis, dafür aber eine bis zu dreifach höhere Geschwindigkeit im Vergleich zu der MLC. Auch der Verschleiß ist bei der MLC höher. Dies liegt darin begründet, dass vor jedem Schreibvorgang die gesamte Zelle gelöscht werden muss. Dabei wird diese von dem Controller kurzzeitig unter eine hohe Spannung gesetzt. Jeder dieser Vorgänge verursacht einen natürlichen Verschleiß. Werden nun mehrere Bits in einer Zelle gespeichert, muss dieser Vorgang im Durchschnitt pro Zelle auch öfters durchgeführt werden.[10][6]
Bei der Wiederherstellung muss in den meisten Fällen der Speicherchip ausgebaut werden und manuell ausgelesen werden. Dabei haben die Datenretter das Problem, dass sie den alten Controller simulieren müssen um die Speicherstruktur der Daten rekonstruieren zu können. Dies wird dadurch erschwert, dass es keine einheitliche Standards gibt und jeder Hersteller seine Daten anders auf dem Speicher ablegt. Durch möglichst gleichmäßige Verteilung der Schreibvorgänge, Erkennung von defekten Blöcken und

Sperrung dieser, dem so genannten *Wear Levelling* wird versucht die Lebensdauer dieser Speicher zu erhöhen. Damit wird allerdings auch gleichzeitig das Auslesen der physikalischen Struktur der Daten erschwert.
Logische Fehler können auf diesen Speichermedien prinzipiell genau so durch Software gelöst werden.

3 Datenrettungslabor

3.1 Phasen der Datenrettung

Grundsätzlich lässt sich die Rettung eines Datenträgers **im** Datenrettungslabor in 3 Phasen aufteilen. Das Zuschicken des defekten Mediums und auch das Zukommenlassen der geretteten Daten wird nicht als eigene Phase gewertet, gehört natürlich dennoch immer zu jedem Rettungsprozess dazu.[7]
Der Versand zum Datenrettungslabor sollte immer gut gepolstert und luftdicht verpackt erfolgen. Denn nur so kann verhindert werden, dass weitere Daten durch Korrosion oder mechanische Einwirkungen verloren gehen.

Phase 1: Analyse
Der erste Teil einer jeden Datenrettung ist die Analyse des Schadens, denn daraus ergibt sich das weitere Vorgehen, welches wiederum maßgeblich für die Kosten der Wiederherstellung ist. Diese Phase findet in den meisten Datenrettungslaboren unentgeltlich statt und der Kunde kann sich nach Erhalt eines Statusberichtes für und gegen die Rettung der Daten entscheiden. Der Statusbericht beinhaltet normalerweise Angaben über die Art des Schadens, eine Prognose welche Daten wiederhergestellt werden können und die dafür anfallenden Kosten.
Während bei logischen Fehlern das Speichermedium direkt angeschlossen werden kann um dann mit einer speziellen Software eine Fehleranalyse durchzuführen, ist die Untersuchung bei physikalischen Fehlern, gerade bei Festplatte komplizierter. Die Wiederinbetriebnahme könnte gerade bei einem Head-Crash die Schäden vergrößern. Um aber trotzdem bei derartigen Fehlern eine Prognose, ohne die Festplatte öffnen zu müssen, geben zu können, haben die Hersteller ein versiegelte Öffnung seitlich integriert. Durch diese Öffnung kann mit Hilfe eines Endoskopes der Zustand der Magnetscheiben und der Schreibarme untersucht werden. Tritt dabei der Fehler nicht zu Tage, so wird im nächsten Schritt die Controller-Elektronik untersucht. Hierfür haben einige Hersteller einen Diagnosemodus integriert mit dessen Hilfe sich die einzelnen Funktion der Festplatte separat testen lassen.

Phase 2: physikalische Rettung
In dieser Phase wird versucht ein exaktes Image Sektor für Sektor von dem wiederherzustellenden Medium zu erzeugen. Dieser Schritt wird immer durchgeführt, auch wenn bei logischen Fehlern oftmals die Daten direkt auf dem Medium wiederhergestellt

[7] außer bei der vorher beschriebenen “Remote Data Recovery”

werden könnten, um sich gegen möglicher Fehler die während des Wiederherstellungsprozesses auftreten zu schützen.
Ist es nicht möglich die Festplatte zu reparieren und sie wieder in Betrieb zu nehmen, so müssen die Magnetscheiben einzeln ausgelesen werden. Hierzu wird der Magnetscheibenstapel aus der Festplatte extrahiert und die einzelnen Scheiben in einer speziellen Maschinen einzeln ausgelesen.
In der norwegischen Datenrettungsfirma IBAS spricht man hierbei von der "Patan Technology" (nähere Infos sh. Einschub). Dieses Verfahren wird in anderen Datenrettungslaboren mit hoher Wahrscheinlichkeit in ähnlicher Weise durchgeführt.

Einschub:[2]*Pattern-Analyser am Beispiel "Patan Technology" der Firma IBAS*
Mit Hilfe eines Pattern-Analysers wird die magnetische Struktur der Magnetscheiben untersucht und ausgelesen. Dabei wird ein Lesekopf der von einer speziellen Software gesteuert wird über die noch intakten Bereiche geführt und die magnetischen Informationen ausgelesen. Die Maschine selber, wie auch die Steuerungssoftware sind Eigenanfertigungen.
Im erster Schritt werden im Reinraum die Pattern von Verunreinigungen befreit. Danach muss der Pattern-Analyser auf die jeweilige Festplatte nach Herstellerangaben eingestellt und kalibriert werden. Nachdem die Maschine eingestellt und der Pattern in dieser befestigt wurde, werden die magnetischen Informationen analog ausgelesen und dann nach eingehender Analyse digitalisiert. Gerade beim Überschreiben von Daten kann es zu "Unsauberkeiten" kommen, da der Schreibkopf nicht immer exakt den Bit an die gleiche Stelle schreibt. So kommt es zu Überlappungen, welche es theoretisch auch möglich machen bereits überschriebene Daten zu rekonstruieren. Ergebnis dieses Prozesses ist, wie vorher bereits beschrieben, ein exaktes Abbild der Festplatte als Image. Fortgefahren wird nun mit der Phase 3, der logischen Rettung.

Phase 3: logische Rettung
Nachdem in der vorherigen Phase ein exaktes Abbild der physikalischen Informationen erstellt wurde, muss nun die logische Verbindung und Struktur wiederhergestellt werden. Bei rein mechanischen Fehlern entfällt dieser Schritt, da die logische Verknüpfung davon nicht betroffen war. Dagegen spielt diese Phase gerade bei Festplattenverbänden oder bei verschlüsselten Laufwerken eine sehr wichtige Rolle.

3.2 Spezial Equipment

Die hohe Wiederherstellungsquote haben die Datenrettungslaboren zum einen ihren qualifizierten Mitarbeitern, aber auch vor allem dem teurem Spezial Equipment zu verdanken.
Wichtigster Bestandteil eines jeden Datenrettungslabors ist seine Sammlung an Ersatzteilen und Festplatten. So kann fast jedes Bauteil einer Festplatte durch ein Neues ersetzt werden und somit die Festplatte wieder in Betrieb genommen werden. Da

die Festplattenhersteller häufig kleine, aber entscheidende Details an ihren Produkten ändern, muss auch jeweils ein Exemplar davon auf Lager sein.
Den Namen Datenrettungs*labor* tragen diese nicht von ungefähr. Gerade Festplatten sind im geöffneten Zustand extrem empfindlich, weshalb auch die Umgebung staubfrei sein muss. Im Labor stehen eine Reihe von Diagnosegeräten zur Verfügung mit denen sich die Medien genau testen lassen um somit auch die Fehlerquelle schnell bestimmen zu können. Zu diesen Diagnosengeräten gehört auch unter anderem ein Endoskop, wie es auch in der Medizin benutzt wird, mit dem sich das Innere einer Festplatte untersuchen lässt ohne diese öffnen zu müssen.

3.3 Arbeit im Reinraum

Gerade Festplatten sind im geöffneten Zustand sehr empfindlich gegen Staub und Partikel aus der Luft. Um weitere Schäden zu verhindern, werden deshalb alle Eingriffe an der Festplatte in einem speziellen Reinraum durchgeführt. Der Reinraum zeichnet sich dadurch aus, dass durch spezielle Filteranlagen die Konzentration luftgetragener Teilchen so gering wie nötig gehalten wird.
Moderne Datenrettungslabore besitzen Reinräume der Klasse 100 (ISO 5). Das bedeutet, dass sich in 1qm Luft nicht mehr als 100 Partikel mit einem Durchmesser von max $0.5\mu m$ befinden dürfen. Die Mitarbeiter selber müssen spezielle Ganzkörperanzüge tragen, damit Hautschuppen und Haare nicht in den Raum geraten.
Aber nicht nur Staubpartikel können die Datenträger beschädigen, auch elektrostatische Entladungen können der empfindliche Elektronik gefährlich werden. Aus diesem Grund wird über Gebläse ionisierte Luft in den Raum geblasen um vor lufttransportierte Spannungen zu schützen.

Abbildung 2: Techniker im Reinraum [3]

3.4 Sicherheitsbestimmungen

Wie im Abschnitt 1.4 schon beschrieben, haben einige Daten einen erheblichen wirtschaftlichen Wert, nicht nur für deren Besitzer, sondern auch für Dritte. Dementsprechend müssen die Daten geschützt werden. Gefahr droht dabei nicht nur durch Attacken von außen, sondern auch durch in Versuchung geratene Mitarbeiter.
Aus diesem Grund gehen die meisten Datenlabore den Weg, dass einmal im Labor angekommene Datenträger nur noch unter einer Vorgangsnummer gelistet sind - alle Hinweise die auf den Eigentürmer schließen lassen werden entfernt. Manche Firmen wie Convar werben sogar mit speziellen Safes die selbst die strengen US Militär Normen erfüllen. Ibas in Norwegen teilt jedem Mitarbeiter nur einen Aufgabenbereich zu. So soll verhindert werden, dass ein Mitarbeiter Überblick über die kompletten Wiederherstellungsprozess eines Datenträgers hat und so eventuell Rückschlüsse auf seinen Eigentümer ziehen kann.
Durch autarke Netzwerke soll der Zugriff auf die Daten von außen unmöglich gemacht werden. Auch bei dem “Remote Data Recovery” Verfahren der Firma Convar wird der gesamte Prozess über eine verschlüsselte Verbindung durchgeführt. Der Transport des Speichermediums selber zum Labor erfolgt auf Wunsch per Kurier.

4 Schlusswort

Bei sensiblen Daten sollte man auf die Hilfe von professionellen Datenrettern zurückgreifen. Jeder selbst durchgeführte Versuch die Daten wieder herzustellen kann zum unweigerlichen Totalverlust führen oder die Rettung noch kostenintensiver machen. Gerade bei Privatanwendern wird immer wieder beobachtet, dass diese aus Angst vor den relativ hohen Kosten versuchen sich selber weiterzuhelfen. So bekommen die Datenrettungsfirmen immer wieder bereits geöffnete Festplatten (teilweise sogar mit Kaffee überschüttet) und gebügelte Magnetbänder angeliefert.
Aber auch die redundante Speicherung der Daten, welche einen sehr guten Schutz vor Datenverlusten bietet, ist relativ teuer und gerade im Privatanwenderbereich wenig verbreitet. Oft bringt aber auch der Anwender durch Unwissen selber seine Daten in Gefahr. So ist das Speichern von Daten auf der primär Partition oder die Benutzung von sehr alten Festplatten fast als fahrlässig einzuschätzen. Oft werden die Auswirkungen eines Datenverlustes unterschätzt und erst bei dessen Eintreten realisiert. Diesen Missstand haben einige Firmen erkannt und so bietet die Firma Freecom unter anderem für Privatpersonen eine Versicherung für Festplatten an. Einmal abgeschlossen und auf jeweils eine Festplatte registriert, werden die Kosten einer professionellen Datenrettung für 3 Jahre übernommen. Auch wenn nicht die gleiche Sicherheit wie bei einer redundanten Speicherung geboten wird, ist es ein Kompromiss zwischen Datensicherheit und zusätzlichen Kosten und somit für knapp 30 Euro eine sehr lohnenswerte Investition.
Die neuen Flashspeicher bieten zwar Sicherheit gegenüber Erschütterungen und mechanischen Defekten, aber wie es oft bei neuen Technologien ist, haben sich noch keine einheitlichen Standards durchgesetzt. Die Datenretter stehen vor dem Problem, dass die Controller von Hersteller zu Hersteller anders programmiert sind und somit auch die physikalische Datenspeicherung auf dem Speicher sich grundsätzlich ändert. Es lässt sich allerdings erwarten, dass dieses Problem mit kommender Verbreitung dieser Speichermedien schwindet.
Zudem lässt sich bei den Nutzern ein wachsendes Bewusstsein für die Bedeutung ihrer Daten beobachten. Immer mehr Nutzer erstellen Backups und die sinkenden Kosten für Datenträger spielen diesem entgegen. Auch die Speicherung im Internet nimmt zu. Dadurch wird die Lagerung der Daten Firmen und ihren Datenspezialisten auferlegt, wodurch die Datensicherheit deutlich erhöht wird.

Literatur

[1] AudioHQ, Compact Disc - Aufbau und Grundlagen, Fehlerkorrektur, Reinigung, Reparatur, Zugriff: 06.12.2010, http://www.audiohq.de/index.php?showtopic=840

[2] ibas, Patan Technology - Advanced Data Recovery, Zugriff: 25.11.2010, http://www.ibas.com/about/technology/patan

[3] ibas, Data Recovery Engineer - working in Cleanroom, Zugriff 19.01.2011, http://gfx.ibas.com/news/pictures/engineer_in_cleanroom.jpg

[4] Kroll Ontrack, Festplatten-Datenrettung, Zugriff: 26.2.2011, http://www.ontrack.de/datenrettung-festplatten

[5] Ponemon Institute, Five Countries: Cost of Data Breach, Zugriff: 06.03.2011, http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2010

[6] proDatenrettung,SSD - Solid State Disks & Daten retten, Zugriff: 29.11.2010, http://www.pro-datenrettung.net/ssd-datenrettung.html

[7] proDatenrettung,Datenrettung USB Stick, Zugriff: 30.11.2010, http://www.pro-datenrettung.net/datenrettung-usb-stick/

[8] TECChannel,Datenrettung: Professionelle Hilfe statt Datenverlust, Zugriff: 21.11.2010, http://www.tecchannel.de/storage/backup/401608/datenrettung_professionelle_hilfe_statt_date

[9] tom's hardware, Tödliches Klacken: Datenrettung nach Festplatten-Crash, Zugriff: 21.11.2010, http://www.tomshardware.de/cbl-datenrettung-festplatten-crash-wiederherstellung,testberichte-236205.html

[10] Wikipedia - die freue Enzyklopädie, MLC-Speicherzelle, Zugriff: 27.11.2010, http://de.wikipedia.org/wiki/MLC-Speicherzelle