Orientierungshilfe

„Sicheres Löschen magnetischer Datenträger“

Grundlagen, Werkzeuge und Empfehlungen aus Sicht des Datenschutzes

erstellt vom Arbeitskreis „Technische und organisatorische Datenschutzfragen“
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder

(Stand: 07.10.2004)

Inhalt

Autor dieser Orientierungshilfe:
Dr. Thomas Reinke
Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg
Stahnsdorfer Damm 77
14532 Kleinmachnow

Zusammenfassung und Empfehlungen

Sowohl aus der Sicht des Datenschutzes als auch der IT-Sicherheit ist beim Löschen von sensiblen oder vertraulichen Daten auf magnetischen Datenträgern zu gewährleisten, dass die Daten sicher, d.h. vollständig und unumkehrbar gelöscht werden. Einfache Löschbefehle des jeweiligen Betriebssystems oder auch das Formatieren des Datenträgers reichen hierzu in der Regel nicht aus, da eine Rekonstruktion der Daten mit frei verfügbaren Softwarewerkzeugen leicht möglich ist. Daten, die sicher gelöscht werden sollen, müssen durch physikalische Maßnahmen (mechanische oder thermische Zerstörung, magnetische Durchflutung des Datenträgers) oder durch mehrmaliges Überschreiben unkenntlich gemacht werden. Beim Löschen durch Überschreiben sind die spezifischen Besonderheiten der Verwaltung und Speicherung von Daten zu berücksichtigen, wie z.B. die Existenz von Sicherheitskopien, von automatisch durch das System oder einzelne Anwendungen angelegten temporären und Auslagerungsdateien oder von Journalen bei bestimmten Dateisystemen.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder gibt in diesem Zusammenhang die folgenden Empfehlungen:

1. Der Problemkreis des sicheren Löschens von Daten erfordert die Sensibilisierung der verantwortlichen Entscheidungsträger, Administratoren, Sicherheits- und Datenschutzbeauftragten sowie jedes einzelnen Nutzers. Dies ist durch geeignete Information und Schulung zu erreichen.
2. Im jeweiligen Verantwortungsbereich sind technisch-organisatorische Maßnahmen festzulegen, die eine sichere Löschung von Daten gewährleisten. Sie sind in das übergreifende Datenschutz- bzw. Sicherheitskonzept zu integrieren. Insbesondere sind Maßnahmen vor der Veräußerung, Vermietung, Aussonderung, Rückgabe, Reparatur und Wartung von Datenträgern zu bestimmen.
3. Die Maßnahmen sind durch konkrete Handlungsanweisungen für das sichere Löschen zu untersetzen. Diese Anweisungen müssen den Schutzbedarf der zu löschenden Daten ebenso berücksichtigen wie den Aufwand und die Kosten für eine mögliche Datenwiederherstellung.
4. Schutzwürdige Daten sind (soweit möglich) bereits in verschlüsselter Form auf dem Datenträger zu speichern. Hierzu sollten verschlüsselte Dateisysteme verwendet werden. Auch für temporäre und Auslagerungsdateien sowie für Sicherheitskopien sollten verschlüsselte Dateisysteme verwendet werden, da diese ebenfalls schutzwürdige Daten enthalten können.
5. Daten auf intakten Datenträgern sind durch das ein- oder mehrmalige, komplette Überschreiben mit Zufallszahlen zu löschen. Hierbei können spezielle Softwarewerkzeuge zum Einsatz kommen. Die Verwendung gleichförmiger Überschreibmuster beim Löschen ist nicht zu empfehlen, da so kein Schutz gegen ausführliche Laboranalysen besteht.
6. Das einmalige, komplette Überschreiben mit Zufallszahlen sollte beim Löschen von Daten jeder Art praktiziert werden. Beim Löschen personenbezogener Daten niedriger oder mittlerer Schutzstufe sollten mindestens 7 Überschreibzyklen ausgeführt werden. Personenbezogene Daten hoher Schutzstufe sollten mit mindestens 33 Überschreibzyklen gelöscht werden.
7. Soll ein noch intakter Datenträger verkauft, vermietet, ausgesondert, zurückgegeben oder einer neuen Nutzung zugeführt werden, ist zuvor der gesamte Datenträger mehrmals komplett mit Zufallszahlen zu überschreiben. Diese Form der Wiederaufbereitung gestattet anschließend die weitere Nutzung des Datenträgers (z.B. die Neuinstallation eines Betriebssystems).
8. Das selektive Löschen einzelner Dateien durch Überschreiben ist meist problematisch. Es eignet sich nur dann, wenn sichergestellt ist, dass keine Kopien der in diesen Dateien enthaltenen Daten an anderen Orten abgelegt wurden (z.B. in temporären Dateien,

Auslagerungsdateien oder Sicherungskopien) oder diese Orte eindeutig bestimmt und auch die Kopien sicher gelöscht werden können. Weiter ist zu gewährleisten, dass die Metadaten der gelöschten Dateien überschrieben werden, falls sie sensible Informationen enthalten.

9. Bei der Festlegung von technisch-organisatorischen Maßnahmen sowie von Handlungsanweisungen für das Löschen durch Überschreiben sind geeignete Softwarewerkzeuge anhand eines Kriterienkatalogs auszuwählen, zu bewerten und für die betreffenden Nutzer bereitzustellen. Die Anwendung der Werkzeuge ist stichprobenartig zu kontrollieren.
10. Defekte Datenträger, deren Daten nicht mehr mit Softwarewerkzeugen überschrieben werden können, sind durch mechanische oder thermische Zerstörung (Disketten, Festplatten) bzw. durch magnetische Durchflutung (Disketten) unbrauchbar zu machen. Um die Zuverlässigkeit der Verfahren zu sichern, ist eine korrekte Anwendung zu gewährleisten.
11. Müssen Datenträger ohne sicheres Löschen der Daten aus der Hand gegeben werden (z.B. Reparatur, Rückgabe an den Hersteller in der Garantiezeit), ist in Abhängigkeit von der Sensibilität der Daten durch vertragliche Regelungen und evtl. mit Schadensersatzansprüchen zu verhindern, dass unerwünschte Informationsflüsse stattfinden oder von Angreifern ausgenutzt werden. Ggf. ist auf Garantieansprüche zu verzichten.

1 Motivation und Ziele

1.1 Motivation

Seit Jahren ist allgemein bekannt, dass in allen gängigen Betriebssystemen beim Aufruf des Befehls zum Löschen einer Datei von einem magnetischen Datenträger (Festplatte, Diskette) nur der Verweis auf die Datei im Inhaltsverzeichnis des Datenträgers gelöscht und der zugehörige Datenbereich als frei markiert wird. Die Daten selbst bleiben jedoch unversehrt an ihrem ursprünglichen Ort, bis sie mehr oder weniger zufällig und ggf. auch nur teilweise durch die Speicherung neuer Dateien überschrieben werden. Weit weniger bekannt ist, dass auch das Formatieren oder das Partitionieren von Festplatten nur einen geringen Teil der Sektoren modifiziert – im Wesentlichen, um Verwaltungsstrukturen für die Partitionen oder das Dateisystem einzurichten.

Die Rekonstruktion von Daten ist häufig relativ einfach durch frei verfügbare Softwarewerkzeuge oder mit etwas detektivischem Spürsinn und Hintergrundwissen durch Nutzung so genannter Disk Editoren möglich. Insbesondere trifft dies zu, wenn keine besonderen Maßnahmen zur Löschung bzw. zum Überschreiben der Daten getroffen wurden. Regelmäßig erscheinen deshalb in der wissenschaftlichen Fachliteratur, populärwissenschaftlichen Zeitschriften, aber auch in der Tagespresse, Rundfunk und Fernsehen Beiträge mit Hinweisen und Empfehlungen zum sicheren Löschen von Daten (siehe z.B. [9], [13], [1], [12], [10]).

Es verwundert deshalb umso mehr, dass ebenso regelmäßig Aufsehen erregend über die erfolgreiche Wiederherstellung von z.T. sensiblen Daten auf vermeintlich gelöschten Festplatten berichtet wird. So fanden z.B. Forscher des Massachusetts Institute of Technology (MIT) unter 158 alten Festplatten, die sie zwischen 2000 und 2002 bei Ebay oder bei Gebrauchtwarenhändlern erworben hatten, nur 12 ohne wiederherstellbare Datenspuren. Auf den anderen Festplatten konnten medizinische Daten, Kreditkarten- und Kontoinformationen oder private Briefe rekonstruiert werden. Auch Teile der Software eines Geldautomaten wurden gefunden [9]. Eine ähnliche Studie, die das schwedische Sicherheitsunternehmen PointSec 2004 durchführte, zeigte bei ca. 70% der untersuchten Festplatten verwertbare Datenreste, u.a. Geschäftsdokumente eines europäischen Finanzdienstleisters [22]. Auch für Ermittlungsbehörden sind alte Festplatten oft eine gute Informationsquelle. Aus diesem Grund wurden z.B. in Deutschland in einigen Landeskriminalämtern spezielle Arbeitsgruppen gebildet, die sich mit derartigen Untersuchungen befassen und helfen, Beweise für Straftaten zu sichern [11].

In der täglichen Arbeit der Datenschutzbehörden gibt es immer wieder Anfragen zur sicheren Löschung bzw. zu Wiederherstellungsmöglichkeiten von Daten auf Datenträgern. Typische Fälle sind z.B. die Aussonderung und Veräußerung von Technik, deren Reparatur durch externe Firmen bei einem Defekt oder die Rückgabe von angemieteter Technik wie Kopierern mit Festplatten. In diesen Fällen sind sensible Daten zuvor möglichst zuverlässig zu löschen. Die jeweils geltenden Datenschutzgesetze legen hier mit entsprechenden Löschvorschriften zusätzlich rechtliche Rahmenbedingungen fest.

Der Aufwand, der für das Löschen zu betreiben ist, muss einerseits den Grad der Sensibilität der Daten berücksichtigen. Andererseits ist zu beachten, dass mittlerweile auch spezielle Mechanismen und Werkzeuge der Computer Forensik bereitstehen – einem Teilgebiet der Informatik, das sich u.a. der Wiederherstellung versehentlich bzw. vorsätzlich gelöschter Daten oder durch Umwelteinflüsse und Katastrophen beschädigter Datenträger widmet (vgl. [20], [11], [17]). Es gibt inzwischen auch Firmen, deren wesentlicher Geschäftszweck die Computer Forensik ist und die mit teilweise erheblichem materiellen und finanziellen Aufwand Daten für ihre Kunden wiederherstellen.

1.2 Ziele und Aufbau des Papiers

Vor diesem Hintergrund stellt sich die vorliegende Ausarbeitung das Ziel, den aktuellen Stand der Technik beim sicheren Löschen von Daten zusammenzufassen und Handlungsempfehlungen bereitzustellen. Sicheres Löschen heißt in diesem Fall vollständiges und nicht umkehrbares Löschen. Auf Grund ihrer Bedeutung und der Häufigkeit ihrer Anwendung erfolgt hierbei eine Einschränkung auf magnetische Speichermedien (d.h. Festplatten und Disketten). Zielgruppe des Papiers sind verantwortliche Entscheidungsträger und Administratoren in Behörden und öffentlichen Einrichtungen sowie interessierte Nutzer. Die Ausführungen basieren auf einem internen Arbeitspapier [19] des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg und entwickeln dieses weiter.

Im Folgenden wird zunächst eine Einordnung der Problematik aus Sicht des Datenschutzes und der IT-Sicherheit im Allgemeinen gegeben (Abschnitt 2). Nach der Zusammenfassung der technischen Grundlagen zur Speicherung von Daten auf magnetischen Datenträgern (Abschnitt 3) werden verschiedene Möglichkeiten zur sicheren Löschung aufgezeigt und bewertet (Abschnitt 4). Abschließend werden ausgewählte, verfügbare Softwarewerkzeuge vorgestellt, die das sichere Löschen durch Überschreiben der Daten realisieren (Abschnitt 5).

2 Aspekte des Datenschutzes und der Datensicherheit

2.1 Anforderungen der Datenschutzgesetze

Gesetzliche Regelungen für das Löschen von Daten finden sich in den Datenschutzgesetzen des Bundes und der Länder. So verlangt z.B. § 20 Abs. 2 Bundesdatenschutzgesetz (BDSG), dass personenbezogene Daten, die durch öffentliche Stellen automatisiert verarbeitet werden, zu löschen sind, wenn ihre Speicherung unzulässig oder ihre Kenntnis für die verantwortliche Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist. Auch für die Datenverarbeitung durch nicht öffentliche Stellen gelten Löschvorschriften (§ 35 BDSG). Weiterhin kann das Löschen von Daten eine geeignete technisch-organisatorische Maßnahme sein, um Unbefugten den Zugriff auf nicht für sie bestimmte Informationen zu verwehren.

Unter Löschen wird hier das Unkenntlichmachen gespeicherter personenbezogener Daten verstanden (§ 3 Abs. 4 Nr. 5 BDSG). Daten werden dann als unkenntlich angenommen, wenn die Informationen nicht länger aus den ursprünglich gespeicherten Daten gewonnen werden können und eine weitere Verarbeitung somit nicht mehr möglich ist.

Gleichzeitig legt § 9 BDSG (bzw. die entsprechenden Regelungen der landesspezifischen Datenschutzgesetze) fest, dass der Aufwand für technisch-organisatorische Maßnahmen in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen soll. Für das Löschen von Daten sind somit insbesondere die Sensibilität der zu löschenden (personenbezogenen) Daten, das Risiko ihrer Wiederherstellung durch Angreifer, die zu erwartende Stärke der Angreifer bzw. der von ihnen betriebene Aufwand zur Datenrekonstruktion zu berücksichtigen.

Durch die sich ständig verbessernden Möglichkeiten der Computer Forensik und die zunehmend freie Verfügbarkeit entsprechender Softwarewerkzeuge sollten an die Löschung von personenbezogenen Daten strenge Anforderungen gestellt werden. Die Stärke der durchgeführten Löschmaßnahmen ist so zu wählen, dass eine Wiederherstellung der Daten für einen Angreifer mit dessen finanziellen oder materiellen Mitteln nicht nur erschwert oder unattraktiv, sondern auch praktisch nicht durchführbar ist.

2.2 Wiederaufbereitung als IT-Sicherheitsmaßnahme

Im Rahmen der IT-Sicherheit ist die Vertraulichkeit eines der Kernziele. Durch Sicherung der Vertraulichkeit sollen Zugriffe auf Daten (und Dienste) nur hierzu Berechtigten möglich sein und unerwünschte Informationsflüsse verhindert werden. Regelmäßig werden deshalb in DV-Systemen entsprechende Sicherheitsmaßnahmen vorgesehen und realisiert, wie z.B. Identifizierung und Authentifizierung, Zugriffskontrolle oder Verschlüsselung.

Auch die Sicherheitsmaßnahme der Wiederaufbereitung von Betriebsmitteln kann helfen, das Sicherheitsziel der Vertraulichkeit zu erreichen. Hierbei geht es darum, dass wiederverwendbare Betriebsmittel wie z.B. Hauptspeicher oder Speicherplatz auf Datenträgern, aber auch Inhalte von Bildschirmmasken, vor der erneuten Zuteilung wiederaufbereitet, d.h. ihre Inhalte gelöscht werden. Dies gilt sowohl für Mehrbenutzerumgebungen als auch für Einzelplatzcomputer, die nacheinander von mehreren Benutzern verwendet werden. Die konkrete Ausgestaltung dieser Sicherheitsmaßnahme muss festlegen, welche Betriebsmittel in die Wiederaufbereitung einbezogen werden und wie bzw. wann die Wiederaufbereitung erfolgt. Wird auf die Wiederaufbereitung verzichtet, ist eine Umgehung der Zugriffskontrolle möglich [8], [16].

Auf Grund dieser Erkenntnisse hat die Wiederaufbereitung als Sicherheitsmaßnahme auch Eingang in Kriterienkataloge zur Bewertung vertrauenswürdiger Systeme gefunden. Hier sind z.B. zu nennen:

- Trusted Computer Systems Evaluation Criteria [7] („Orange Book“): Für eine Bewertung nach der (niedrigen) Stufe C2 sind die Anforderungen des Object Reuse zu erfüllen. Dabei ist sicherzustellen, dass keine Informationen (auch nicht in verschlüsselter Form!), die in Speicherobjekten hinterlassen wurden, für Unberechtigte zugänglich werden.
- Deutsche und Europäische IT-Sicherheitskriterien [14], [15]: Die Funktionalitätsklassen F2 bzw. F-C2 dieser Kataloge sind direkt aus den funktionalen Anforderungen der TCSEC-Klasse C2 abgeleitet. Sie fordern, dass alle Speicherobjekte vor ihrer Wiederverwendung so aufbereitet werden, dass keine Rückschlüsse auf frühere Inhalte möglich sind.
- Common Criteria [18]: Zur Festlegung von Schutzprofilen und Bewertung von Systemen bieten die CC die Schutzklasse FDP „User Data Protection“ mit der Schutzfamilie RIP „Residual Information Protection“ an. Hierin wird u.a. gefordert, dass gelöschte Informationen nicht mehr zugänglich sind und neu erzeugte Objekte keine alten Informationen mehr enthalten.

Darüber hinaus enthält auch das IT-Grundschutzhandbuch [2] (GSHB) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) Maßnahmen, die sich auf die Löschung von Daten beziehen. Dies sind z.B.

- M 2.167 – Sicheres Löschen von Datenträgern: benennt Varianten des Löschens und enthält einen Vorschlag zum Löschen magnetischer Datenträger durch Überschreiben (siehe Abschnitt 4.2 dieses Papiers),
- M 4.32 – Physikalisches Löschen der Datenträger vor und nach Verwendung: enthält Maßnahmen zum Löschen bei Nutzung des Datenträgeraustauschs,
- M 4.56 – Sicheres Löschen unter Windows NT und 95: berücksichtigt Eigenschaften des Dateisystems NTFS und den Umgang mit dem „Papierkorb“ auf dem Windows Desktop.

Zusammenfassend lässt sich somit feststellen, dass die Entwicklung und Nutzung von Verfahren zum sicheren Löschen von Daten sowohl aus Datenschutzgründen als auch aus Gründen der IT-Sicherheit von großer Bedeutung ist.

3 Grundlagen des Speicherns von Daten auf magnetischen Datenträgern

Bevor im Abschnitt 4 die Möglichkeiten für das sichere Löschen von Daten auf magnetischen Speichermedien erörtert werden, sollen zunächst die wichtigsten Grundlagen ihrer Speicherung zusammenfassend dargestellt werden. Dies dient auch der Vereinbarung und einheitlichen Verwendung von Begriffen.

3.1 Festplattengeometrie

Magnetische Speichermedien bestehen im Wesentlichen aus einer (bei Disketten) oder mehreren (bei Festplatten) rotierenden Scheiben bzw. Platten, die in einem Stapel angeordnet sind und eine magnetisierbare Oberfläche besitzen. Über jeder Oberfläche schwebt ein Schreib-/Lesekopf, der magnetische Flusswechsel auf der Plattenoberfläche in einen elektrischen Stromfluss umwandelt (Lesen) bzw. umgekehrt (Schreiben). Alle Köpfe sind starr miteinander verbunden und ragen kammartig in den Plattenstapel hinein. Die einzelnen Platten sind in konzentrische Spuren unterteilt, die ihrerseits in Sektoren gegliedert werden. Jeder Sektor fasst 512 Bytes und ist die kleinste adressierbare Einheit der Festplatte. Die Zusammenfassung aller Sektoren, die übereinander im Plattenstapel liegen, heißt Zylinder. In einem Zylinder können alle Sektoren gleichzeitig ohne Neupositionierung der Köpfe gelesen bzw. geschrieben werden.

Anstelle der Adressierung von Sektoren durch die Angabe von Zylinder-, Kopf- und Sektornummer (CHS-Adressierung) verwenden moderne Festplatten eine logische Adressierung, bei der alle Sektoren der Festplatte von 0 beginnend durchnummeriert werden (LBA – Logical Block Adressing). Damit werden einerseits Beschränkungen des BIOS (Basic Input Output System) zur Ansteuerung der Hardware umgangen. Andererseits kann so auch dem Umstand Rechnung getragen werden, dass in äußeren, längeren Spuren mehr Sektoren untergebracht werden können als in inneren, kürzeren Spuren.

3.2 Datencodierung und Aufzeichnungsverfahren

Zur Speicherung von Daten wird deren binäre Repräsentation als Folge von 0- und 1-Werten in Form magnetischer Flusswechsel auf der Plattenoberfläche aufgezeichnet. Wichtig ist hierbei, dass auch sehr lange Abschnitte mit konstanten Bitwerten (z.B. 100 mal Wert 0) regelmäßig zu Flusswechseln führen müssen. Hierzu werden so genannte Taktbits in den Bitstrom eingefügt. Auf diese Weise können Synchronisationsprobleme beim Lesen bzw. Schreiben auf der Festplatte vermieden werden.

In der Vergangenheit haben sich eine Reihe von Codierungsverfahren entwickelt, die für die Aufzeichnung von Bitfolgen als Folgen magnetischer Flusswechsel Verwendung finden. Ältere Verfahren nutzen z.B. die Run-Length Limited (RLL)-Codierung. Sie unterscheiden sich darin, wie groß der Abstand zwischen Flusswechseln minimal sein muss bzw. maximal sein darf. Das einfachste dieser Verfahren ist (1,3) RLL. Es legt fest, dass bei beliebiger Ausgangsbitfolge der minimale Abstand zwischen zwei Flusswechseln 1 und der maximale Abstand 3 ist. Andere Verfahren sind z.B. (1,7) RLL, (2,7) RLL und (3,9) RLL.

Mit dem Fortschreiten der technischen Möglichkeiten konnte eine zunehmend dichtere Packung von Daten auf Festplatten erreicht werden. Neue und komplexe Codierungsverfahren wurden entwickelt, fehlerkorrigierende Codes verwendet und statistische Methoden genutzt. Einige Beispiele sind PRML (Partial Response Maximum Likelihood), EPRML (Extended Partial Response Maximum Likelihood), EEPRML (Extended Extended Partial Response Maximum Likelihood), Trellis Codes oder MTR (Maximum Transition Run) Codes

(siehe auch [19]). Ergebnis dieser Entwicklung ist, dass heute eine Vielzahl verschiedener Aufzeichnungsverfahren für Festplatten konkurrieren, die z.T. herstellerspezifisch verbessert wurden, proprietäre Erweiterungen erhielten oder durch Patente geschützt sind. Es ist deshalb auch prinzipiell unmöglich, ein einziges, universelles und für alle Festplatten und Codierungsarten optimales Verfahren zum sicheren Löschen durch Überschreiben anzugeben [19].

3.3 Dateien und Dateisysteme

Logisch zusammengehörende Daten werden in Dateien zusammengefasst. Das jeweilige Betriebssystem kann Dateien unter Benutzung des BIOS (Ansteuerung der Hardware) und der spezifischen Codierungsverfahren auf einem Datenträger speichern bzw. von einem Datenträger lesen. Die Organisation von Dateien auf dem Datenträger wird durch ein Dateisystem bestimmt. Insbesondere legt ein Dateisystem Verwaltungsstrukturen fest, die einen effizienten Umgang auch mit größeren Dateien zulassen oder eine schnelle Dateisuche ermöglichen. Bekannte Dateisysteme sind z.B. für Windows-Betriebssysteme FAT, FAT32 oder NTFS und für Linux/Unix-Betriebssysteme ext2, ext3, ReiserFS oder JFS.

Die Einrichtung eines Dateisystems muss vor seiner ersten Benutzung erfolgen. Die Vorbereitungsphase beinhaltet das Partitionieren und das Formatieren. Beim (optionalen) Partitionieren werden größere Festplatten in mehrere kleinere Partitionen aufgeteilt. Jede dieser Partitionen kann genau ein Dateisystem enthalten. Durch das Formatieren der Partition (bzw. des Datenträgers bei nur einer Partition) wird das Dateisystem eingerichtet. Zu beachten ist, dass im Allgemeinen weder beim Partitionieren noch beim Formatieren die Datenbereiche selbst in großem Umfang modifiziert werden. Vielmehr werden nur Verwaltungsinformationen in wenige ausgewählte Sektoren geschrieben (z.B. Partition Table, Boot Sector, File Allocation Table, Superblock, Inode Tables) sowie ein Test aller Sektoren auf Lesbarkeit durchgeführt.

Die kleinste Verwaltungseinheit eines Dateisystems ist ein Cluster (Block). Ein Cluster fasst mehrere physische Sektoren der Festplatte zusammen. Gängige Clustergrößen liegen bei Festplatten zwischen 1 und 8 kBytes. Da ein Cluster die kleinste Adressierungseinheit des Betriebssystems ist, muss jede Datei mindestens den Platz eines Clusters einnehmen, auch wenn sie nur wenige Bytes groß ist. Für Dateien, deren Größe nicht ein Vielfaches der Clustergröße ist, entsteht somit ein Verschnitt, d.h. ungenutzter Platz auf der Platte (der so genannte „File Slack“).

Alle gängigen Betriebssysteme realisieren das Löschen von Dateien aus Gründen der schnelleren Reaktionszeit so, dass die zu löschende Datei nur in den Verwaltungsstrukturen des Dateisystems als „gelöscht“ und die von ihr belegten Cluster als „frei“ markiert werden (logisches Löschen). Die eigentlichen Daten bleiben solange unangetastet, bis sie mehr oder weniger zufällig und meist unvollständig durch neue Dateien überschrieben werden. Auch kann der Effekt auftreten, dass die neue Datei im letzten Cluster nur wenig Platz braucht und somit Reste einer alten Datei nicht überschrieben werden, im File Slack liegen und über geeignete Werkzeuge zugreifbar sind.

3.4 Besondere Dateien

Für die Belange des sicheren Löschens von Daten sind in Abhängigkeit von der konkreten Systemkonfiguration eine Reihe spezieller Dateien sowie Besonderheiten, die mit der Art des Speicherns zusammenhängen, zu beachten. Sie sind in der folgenden Aufzählung benannt:

- temporäre Dateien, Arbeits- und Sicherungskopien: Viele Anwendungsprogramme (z.B. Textverarbeitungen, Editoren oder Packprogramme) legen während ihrer Arbeit temporär Dateien an, in denen auch nutzerspezifische Daten gespeichert werden. Im günstigsten

Fall werden temporäre Dateien bei Beendigung des Programms automatisch gelöscht, allerdings in der Regel nur mit dem normalen Löschbefehl des Betriebssystems. Die Daten sind somit leicht wiederherstellbar. Auch lassen sich viele Programme so konfigurieren, dass die vorletzte Version einer Datei automatisch als Sicherungskopie aufbewahrt wird (z. B. durch die Erweiterung .bak oder .sik des Dateinamens erkennbar). Der Nutzer muss sich selbst um das sichere Löschen dieser Dateien kümmern. Gleiches gilt natürlich für die Originaldateien bei einer manuell initiierten Verschlüsselung oder Kompression sowie beim Aufruf von Betriebssystemkommandos zum Kopieren (copy) oder Bewegen (move) von Dateien.

- Auslagerungsdateien, Swap Files, Hibernation Files: Betriebssysteme lagern regelmäßig bestimmte Bereiche des Arbeitsspeichers zeitweise auf die Festplatte aus. Hierzu werden spezielle Dateien (Windows: pagefile.sys) oder Partitionen (Linux: swap-Partition) genutzt. Da in diesen Auslagerungsbereichen Speicherauszüge enthalten sind, können dort auch nutzerspezifische Daten liegen. Sollen Dateien sicher gelöscht werden, sind somit auch die Auslagerungsbereiche zu löschen.
  Eine weitere Besonderheit ist der so genannte Hibernation Modus, der häufig bei Laptops zum schnelleren Beenden und Starten des Rechners genutzt wird. In diesem Modus wird der aktuelle Zustand des Rechners in einem Hibernation File (oder einer entsprechenden Partition) gespeichert. Der Ort der Speicherung kann auch der Auslagerungsbereich sein. Für das Löschen gilt bzgl. des Hibernation Files das für Auslagerungsbereiche Gesagte.
- Journale in journalisierenden Dateisystemen: Moderne Dateisysteme führen während ihrer Arbeit ein Journal, in dem alle Dateioperationen protokolliert werden. Dieses Protokoll ermöglich nach einem Systemabsturz (z.B. durch Stromausfall) eine schnelle Wiederherstellung der Konsistenz des Dateisystems. Für das Löschen von Dateien ist die Eigenschaft solcher Dateisysteme relevant, bei entsprechender Konfiguration im Journal nicht nur die Dateioperationen, sondern auch die zu schreibenden Daten selbst zu protokollieren. Das Journal kann somit nutzerspezifische Daten enthalten.
- RAID-Systeme: Hierbei werden mehrere Partitionen auf verschiedenen Festplatten durch geeignete Hard- oder Software verknüpft und Daten redundant abgespeichert. Die Redundanz ermöglicht einen schnelleren (weil parallelen) Zugriff und eine höhere Robustheit des Speichersystems. RAID-Systeme können Daten einer Datei auf verschiedene Festplatten verteilen, Festplatten/Partitionen spiegeln oder Daten mit zusätzlichen Paritätsinformationen für eine Datenkorrektur versehen. Besondere Maßnahmen zum sicheren Löschen müssen auch die evtl. eingesetzten RAID-Systeme berücksichtigen.
- externe Backups: Letztlich ist für das sichere Löschen von Daten auch die Existenz externer Backups zu beachten. Diese können z.B. auf Magnetbändern, separaten Festplatten, CDs oder DVDs vorliegen. Durch geeignete organisatorische Maßnahmen ist sicherzustellen, dass Daten, die auf Primärdatenträgern gelöscht werden, auch von Backups entfernt oder zumindest gesperrt werden. Da es sich hierbei jedoch nicht um die Löschung in einem (physisch abgegrenzten) Computersystem handelt, wird dieser Fall im weiteren Verlauf der Darstellung ausgeklammert.

4 Möglichkeiten für das sichere Löschen

Die wesentlichen Probleme beim sicheren (d.h. beim vollständigen und nicht umkehrbaren) Löschen von Daten auf magnetischen Datenträgern ergeben sich aus den im letzten Abschnitt dargestellten Eigenschaften des Speicherns:

- Der Aufruf des Löschbefehls löscht nur den Dateieintrag in den Verwaltungsstrukturen des Dateisystems, nicht aber die eigentlichen Daten.
- Alte Daten werden mehr oder weniger zufällig mit neuen Daten überschrieben. Dies geschieht meist nur unvollständig.

- Kopien von Daten können an verschiedenen Orten vorhanden sein, deren Kenntnis und Kontrolle sich dem Nutzer z.T. verschließt.

Für das sichere Löschen sind deshalb Verfahren und Mechanismen erforderlich, die über die Standardverfahren zur (logischen) Löschung, wie sie vom jeweiligen Betriebssystem angeboten werden, hinausgehen. Diese Verfahren und Mechanismen müssen bei sehr sensiblen Daten mit hohem Schutzbedarf außerdem gegenüber den fortschreitenden Möglichkeiten der Computer Forensik sicher sein.

Prinzipiell lassen sich für das sichere Löschen zwei Varianten unterscheiden: einerseits der Einsatz physikalischer Maßnahmen mit einer mechanischen, thermischen oder magnetischen Behandlung des gesamten Datenträgers und andererseits das ein- oder mehrmalige, gezielte Überschreiben von Daten.

4.1 Physikalische Maßnahmen

Physikalische Maßnahmen zum Löschen von Daten sind die mechanische, thermische und magnetische Behandlung des gesamten Datenträgers. Diese Verfahren haben die gemeinsame Eigenschaft, dass nach ihrer Anwendung der Datenträger im Allgemeinen zerstört und nicht mehr verwendbar ist. Sie erfüllen damit nicht die Anforderung der Wiederaufbereitung von Betriebsmitteln.

Allerdings stellen die physikalischen Maßnahmen die einzige Möglichkeit des Löschens von Daten dar, falls der Einsatz von Softwarewerkzeugen zum Löschen durch Überschreiben fehlschlägt. Dies kann auf Grund mechanischer oder elektrischer Defekte des Datenträgers (Fehler in der Steuerung oder Justierung des Schreib-/Lesekopfs, elektrischer Kurzschluss u.a.) oder wegen Fehlern in der magnetisierbaren Oberfläche der Fall sein.

Mechanische Zerstörung
Bei dieser Maßnahme sind die einzelnen Platten/Scheiben einer Festplatte bzw. Diskette so zu zerkleinern, dass aus den verbleibenden Resten keine (sinnvollen) Informationen mehr gewonnen werden können. Damit ist für die Güte des Verfahrens die Größe der entstehenden Partikel entscheidend. Auf Grund der hohen Packungsdichte von Daten auf magnetischen Datenträgern kann davon ausgegangen werden, dass die in der DIN-Norm 32757 für die datenschutzgerechte Vernichtung von Datenträgern aus Papier, Film, Kunststoff oder Metall geforderte Streifenbreite von höchstens 2 mm bzw. eine Partikelgröße von höchstens 4 mm x 80 mm nicht ausreichend ist. Auch die im Hinweisblatt Nr. 11 des BSI [3] zur Umsetzung des § 12 der VS IT-Richtlinien des Bundesministerium des Innern geforderte Partikelgröße von 30 mm^2 für die Vernichtung von Magnetbändern und Disketten mit gespeicherten Verschlusssachen ist kritisch zu betrachten. Als sicher gelten dagegen das Pulverisieren der Scheiben oder das Abschleifen der Magnetschicht von der Oberfläche.

Insgesamt ist die mechanische Zerstörung wegen des hohen Aufwands im Vergleich zur erzielbaren Sicherheit nur eingeschränkt zu empfehlen.

Thermische Zerstörung
Die thermische Zerstörung nutzt die Erkenntnis, dass ein Material irreversibel seine magnetischen Eigenschaften verliert, wenn es über die so genannte Curie-Temperatur erhitzt wird. Für reines Eisen liegt diese Temperatur bei über 750 °C.

Für die thermische Behandlung von Festplatten ist zu sichern, dass die Curie-Temperatur über den gesamten Stapel der magnetisierbaren Scheiben und auch im Innern der Festplatte erreicht wird. Entsprechend ist die Zeitdauer der Hitzeeinwirkung zu verlängern, um die beabsichtigte Wirkung zu erzielen. Zusätzlich sichern lässt sich das Verfahren, indem eine

Kombination aus mechanischer Zerstörung und anschließendem Einschmelzen eingesetzt wird. Bei Anwendung des thermischen Verfahrens für Disketten wird vor dem Erreichen der Curie-Temperatur im Allgemeinen die Kunststofffolie (als Träger der magnetischen Schicht) schmelzen bzw. verbrennen.

Magnetische Durchflutung
Das Löschen von Datenträgern mittels magnetischer Durchflutung erfolgt unter Einsatz von speziellen Löschgeräten, so genannter Degausser. Diese setzen den magnetischen Datenträger einem externen, magnetischen Wechselfeld mit abnehmender Amplitude aus, durch dessen Wirkung die ursprünglich auf dem Datenträger enthaltenen Informationen gelöscht werden. Die Norm DIN 33858 spezifiziert Anforderungen an Degausser. Zu beachten ist, dass Degausser auch eine evtl. vorhandene Servo-Spur auf dem Datenträger durchfluten (z.B. bei Disketten), womit dessen weitere Benutzung im Allgemeinen nicht möglich ist.

Ähnlich wie bei der thermischen Zerstörung ist der Einsatz von Degaussern für Festplatten kritisch zu beurteilen, da auf Grund des unterschiedlichen konstruktiven Aufbaus von Festplatten keine zuverlässigen Aussagen über die Wirksamkeit des Verfahrens getroffen werden können. Insbesondere können die Innenbereiche des Plattenstapels nach einer magnetischen Durchflutung noch verwertbare Informationen enthalten. In [3] werden darum Degausser für die Löschung von Festplatten als prinzipiell ungeeignet angesehen. Für Disketten können sie jedoch Verwendung finden.

4.2 Löschen durch Überschreiben

Daten auf magnetischen Datenträgern können durch Überschreiben vollständig und nicht wiederherstellbar gelöscht werden. Die Datenträger selbst sind nach dem Überschreiben weiter benutzbar (Wiederaufbereitung). Sie können auch mit ruhigem Gewissen entsorgt, verkauft oder im Falle der Vermietung zurückgegeben werden. Zu klären sind in diesem Zusammenhang allerdings Fragen nach den Datenmustern, mit denen überschrieben werden muss, sowie nach der Anzahl der Überschreibvorgänge.

Überschreibmuster und Überschreibzyklen
Ziel des Löschens durch Überschreiben ist es, die Weissschen Bezirke der magnetisierbaren Oberfläche möglichst oft umzuorientieren, so dass der verbleibende Restmagnetismus keine Aussagen über die ursprünglichen Daten mehr zulässt. Dabei ist zu beachten, dass mit Hilfe moderner Werkzeuge und Verfahren der Computer Forensik das einmalige und z.T sogar mehrmalige Überschreiben von Datenträgern mit definierten Überschreibmustern rückgängig gemacht und die Ausgangsdaten reproduziert werden können. Hierzu wird die Eigenschaft der magnetischen Flussstärke als analoger Größe ausgenutzt. Vereinfacht bedeutet dies: Beim Überschreiben einer 1 mit einer 1 ist die resultierende Flussdichte höher als beim Überschreiben einer 0 mit einer 1. Die Wiederherstellung der Ausgangsdaten verlangt jedoch meist einen erheblichen materiellen und finanziellen Aufwand und den Einsatz spezieller Geräte wie z.B. Scanning Probe- oder Magnetic Force-Mikroskopen (SPMs, MFMs) [20].

Einige frühe Ansätze des sicheren Löschens durch Überschreiben versuchten, alle denkbaren Codierungen von Daten zu verwenden, um Bitfolgen für optimale Überschreibmuster zu bestimmen. Diese Ansätze waren somit stets abhängig von der konkret verwendeten Codierung und dem Aufzeichnungsverfahren einer Festplatte (bzw. eines Festplattentyps wie z.B. (1,3), (1,7) oder (2,7) RLL). Um das Löschen auch für verschiedene Festplattentypen zu ermöglichen, wurden die unterschiedlichen Überschreibmuster einfach hintereinander angewendet (oder in zufälliger Reihenfolge). Dies resultierte z.B. bei dem bekanntesten aller Verfahren nach Gutmann in insgesamt 35 Überschreibzyklen [13] – auch wenn das für die wirklich verwendete Codierung einer konkreten Festplatte völlig überflüssig war.

Die fortschreitende technische Entwicklung mit der Zunahme der Speicherdichte und der Verbesserung der Aufzeichnungsverfahren von Festplatten führte dazu, dass die anhand möglicher Codierungen festgelegten Überschreibmuster heute nur noch geringe Bedeutung haben. Insbesondere für moderne Festplatten mit einem großen Speicherumfang und für Festplatten mit nicht bekannten, proprietären Aufzeichnungsverfahren reicht die Verwendung von (gleichverteilten) Zufallszahlen für das Löschen durch Überschreiben aus. Dies wird auch von Gutmann auf seiner Webseite bestätigt [13].

Allerdings sollte auch bei der Nutzung von Zufallszahlen als Überschreibmuster die Anzahl der Überschreibzyklen groß genug gewählt werden, damit ausführliche Laboranalysen keine sensiblen Daten mehr zu Tage fördern können. Wahrscheinlichkeitstheoretische Betrachtungen in [19] zeigen, dass 33 Schreibvorgänge mit Zufallszahlen ausreichen, um mit einer Wahrscheinlichkeit von 0,99 in jeden Bereich der Festplatte mindestens einmal die Muster 010 und 101 zu schreiben. Bereits 7 Wiederholungen reichen aus, damit mit einer Wahrscheinlichkeit von 0,99 jeder Bereich der Festplatte mindestens einmal umorientiert wird. Praktische Untersuchungen zeigen darüber hinaus, dass bereits ein einziger Durchlauf für das sichere Löschen durch Überschreiben genügt, wenn nur einfache Wiederherstellungsmöglichkeiten genutzt werden können (z.B. gängige Softwarewerkzeuge) und ausführliche Laboranalysen mit speziellen Geräten aus Zeit- und/oder Kostengründen nicht durchführbar sind [1].

Ausgewählte Löschverfahren im Überblick

Die folgende Tabelle gibt einen Überblick über einige bekannte Löschverfahren und Löschstandards, fasst ihre wesentlichen Eigenschaften zusammen und bewertet sie. Im Anschluss folgen einige Erläuterungen. Für ausführliche Darstellungen wird auf die jeweils angegebene Originalliteratur oder auf [19] verwiesen.

Tabelle 1: Überblick über Löschverfahren

Verfahren	Anzahl der Überschreib-vorgänge	Verwendung von Zufalls-zahlen	Berücksichtigung verschiedener Codierungen	Schutz gegen ausführliche Laboranalysen
Single Pass 0 oder 1	1	nein	nein	sehr gering
BSI GSHB	4 bis 6	nein	nein	gering
VS IT-Richtlinien	7	nein	nein	gering
DoD 5220.22-M	3	ja (einmal)	nein	gering
DoD 5220.22-M ECE	7	ja (dreimal)	nein	mittel
Gutmann	35	ja (achtmal)	ja (27-mal)	sehr hoch
Pfitzner	33	ja (33-mal)	nein	sehr hoch

Die einfachste Form des Löschens ist das einmalige Überschreiben der Daten (Single Pass) auf Bitebene mit dem Wert 0 oder 1. Dieses Verfahren hält nur der Wiederherstellung mit gängigen Softwarewerkzeugen stand, nicht jedoch einer Analyse des Datenträgers in einem Forensiklabor. Die gleiche Sicherheit erreicht man auch bei Verwendung eines konstanten Überschreibmusters oder bei einmaligem Überschreiben mit Zufallszahlen.

Sowohl das Grundschutzhandbuch des BSI [2] als auch die Hinweise zum Löschen von Verschlusssachen [3] empfehlen ein mehrmaliges Überschreiben von Daten mit festen, zueinander komplementären Bitmustern. Das Grundschutzhandbuch schlägt vor, ein nichtgleichförmiges Muster wie z.B. den Hexadezimalwert C1 (entspricht binär 1100 0001) im ersten Durchgang und anschließend dessen Komplement – hier 3E (binär 0011 1110) – zu verwenden, damit jedes Bit einmal geändert wird. Die Überschreibprozedur sollte zwei-, besser dreimal wiederholt werden. Die Hinweise zum Löschen von Verschlusssachen

empfehlen das sechsmalige Überschreiben mit den hexadezimalen Mustern 00 und FF und das anschließende Überschreiben mit dem hexadezimalen Muster 55 oder AA. Der letztgenannte Algorithmus findet auch in dem Werkzeug VS Clean Verwendung, dass vom BSI offiziell für den öffentlichen Dienst empfohlen wird.

Die Wiederholung des Überschreibvorgangs erhöht zwar die Sicherheit des Löschens gegenüber dem Single Pass-Verfahren, allerdings ist durch die Verwendung fester Überschreibmuster eine Rekonstruktion der Originaldaten aus analogen Signalen möglich (wenn auch mit erheblichem Aufwand). Beide Vorschläge berücksichtigen auch nicht die unterschiedlichen Aufzeichnungsverfahren magnetischer Datenträger.

Die Empfehlungen des US-Verteidigungsministeriums finden sich in den Standards DoD 5220.22-M bzw. 5220.22-M ECE [6]. In der ersten Variante werden die Daten zunächst mit einem festen Wert, dann dessen Komplement und im Anschluss mit Zufallszahlen überschrieben. Das zweite Verfahren wendet die erste Variante zweimal an und überschreibt die Daten zwischen den beiden Durchläufen mit Zufallszahlen. Beide Empfehlungen berücksichtigen zwar ebenfalls nicht die unterschiedlichen Aufzeichnungsverfahren, erhöhen die Sicherheit gegenüber dem Single Pass jedoch durch die Wiederholungen und zusätzlich durch das Überschreiben mit Zufallszahlen.

Gutmann hat in [13] ein Löschverfahren angegeben, dass die möglichen Codierungen bei MFM-, (1,7) RLL- und (2,7) RLL-Festplatten bei der Definition der Überschreibmuster berücksichtigt. Daraus ergeben sich insgesamt 27 Überschreibzyklen. Darüber hinaus werden 8 Zyklen mit Zufallszahlen ausgeführt. Das Verfahren kann als sehr sicher auch gegenüber ausführlichen Laboranalysen eingeschätzt werden. Insbesondere ältere Datenträger, welche die genannten Aufzeichnungsverfahren nutzen, können hiermit irreversibel gelöscht werden. Auch der Vorschlag von Pfitzner [19] kann der Gruppe der sehr sicheren Verfahren zugeordnet werden. Hier wird durch wahrscheinlichkeitstheoretische Betrachtungen die erforderliche Anzahl an Überschreibzyklen bestimmt (s.o.).

Zusammenfassend können für das Löschen durch Überschreiben aus Sicht des Datenschutzes die folgenden, prinzipiellen Empfehlungen gegeben werden:

- Alle Daten sollten durch ein- oder mehrmaliges Überschreiben gelöscht werden. Bei den Überschreibmustern sollten Zufallszahlen gegenüber festen Überschreibmustern bevorzugt werden.
- Beim Löschen von personenbezogenen Daten mit niedriger oder mittlerer Schutzstufe ist die Anzahl der Überschreibzyklen zu erhöhen. Nach 7 Wiederholungen besteht eine hinreichende Sicherheit gegen die Wiederherstellung der Originaldaten.
- Personenbezogene Daten mit hoher Schutzstufe sollten durch mindestens 33 Überschreibzyklen gelöscht werden.

Weiterhin ist darauf hinzuweisen, dass durch Anwendung geeigneter Verschlüsselungsmechanismen bereits bei der Speicherung der Originaldaten auf einem Datenträger deren Wiederherstellung nach dem Löschen durch Überschreiben zusätzlich erschwert werden kann. In den letzten Jahren wurden hierzu verschiedene Möglichkeiten entwickelt, die von der (manuellen oder automatischen) Verschlüsselung einzelner Dateien über die Nutzung verschlüsselter Dateicontainer (z.B. PGP File bzw. Disk [4]) bis hin zu vollständig und für den Benutzer transparent verschlüsselten Dateisystemen (z.B. Encrypted File System für Windows 2000 und XP [5] und für Linux [21]) reichen. Die verschlüsselte Speicherung der Daten bietet auch einen guten Schutz bei Diebstahl des Datenträgers bzw. des ganzen Computers.

4.3 Weitere Bemerkungen zum Löschen durch Überschreiben

Die Ausführungen im Abschnitt 3.4 bedeuten in letzter Konsequenz, dass das Löschen einzelner Dateien durch Überschreiben den Nutzer (bzw. den Verantwortlichen) in einer meist trügerischen Sicherheit wiegt. Die Existenz von Sicherheitskopien, von temporären Dateien, Auslagerungsdateien, Journalen bei bestimmten Dateisystemen u.a. kann zu unerwünschten Informationsflüssen führen, wenn einem Angreifer die Wiederherstellung sensibler Daten aus diesen besonderen Dateien gelingt. Das Aufspüren sämtlicher möglicher Kopien der Daten ist nicht nur mühselig und zeitaufwändig, sondern auch fehlerträchtig. Deshalb ist in der Regel das Löschen kompletter Festplattenpartitionen bzw. kompletter Festplatten dem Löschen einzelner Dateien vorzuziehen. Werden Daten durch Nutzung eines RAID-Systems auf mehrere Festplatten verteilt, gilt diese Empfehlung für alle beteiligten Festplatten.

Weiterhin ist zu bedenken, dass das Überschreiben der Datenbereiche einer Datei nicht die zugehörigen Verwaltungsinformationen im Dateisystem löscht. Unter Umständen sind jedoch bereits Dateinamen, Zeitstempel für Erzeugung oder Änderung einer Datei, Zugriffsrechte u.ä. sensible Daten. Um diese Metainformationen zu verschleiern, könnte man die betreffende Datei mehrfach umbenennen, die Zeitstempel ändern usw. Allerdings ist auch hier das komplette Überschreiben der gesamten Partition bzw. Festplatte der einfachere und auch sicherere Weg.

Zusätzliche Probleme können sich aus konstruktions- und herstellerspezifischen Besonderheiten von Datenträgern ergeben. Zu nennen sind hier beispielsweise Festplattencaches sowie das Management schlechter Sektoren. Caches sind Zwischenspeicher für zu lesende bzw. zu schreibende Daten, die zur Steigerung der Performanz und des Durchsatzes der Plattenzugriffe eingesetzt werden. Sie können als Hardware- oder Softwarecache realisiert sein. Für das Löschen durch Überschreiben ist zu gewährleisten, dass der Cache deaktiviert und nach jedem Schreibzyklus vollständig geleert wird, damit die überschreibenden Daten auch wirklich auf dem Datenträger landen (auch entsprechend der gewählten Anzahl an Überschreibzyklen) und nicht nur im Cache jeweils ausgetauscht werden.

Defekte Sektoren werden meist schon durch die herstellerspezifische Festplattenverwaltung gekennzeichnet und ausgeblendet, d.h. von der weiteren Verwendung ausgeschlossen. Sie sind damit für das Betriebssystem und die Anwendungen nicht mehr ansprechbar. Lösch- und Überschreibprogramme verfehlen deshalb bei defekten Sektoren ihre Wirkung. Wurden allerdings schon Daten in den Sektoren gespeichert, bevor der Defekt auftrat, können ausführliche Laboranalysen diese Daten wiederherstellen. Auswege bieten hier Werkzeuge zur Low-Level-Behandlung von Festplatten/Sektoren, die jedoch herstellerspezifisch und nur z.T. öffentlich verfügbar sind. Alternativ ist auch die Anwendung physikalischer Maßnahmen zum sicheren Löschen möglich.

5 Ausgewählte Werkzeuge zum sicheren Löschen

5.1 Anforderungen an Löschwerkzeuge

Die bisherigen Erkenntnisse gestatten es, eine Reihe von Anforderungen zu definieren, denen Softwarewerkzeuge für das sichere Löschen durch Überschreiben gerecht werden sollten. Sie können auch als Auswahlkriterien bei der Beschaffung eines konkreten Werkzeugs dienen. Folgende Anforderungen lassen sich benennen:

- Auswahl der zu löschenden Objekte: einzelne Dateien, temporäre Dateien, Auslagerungsspeicher, ungenutzter Platz auf dem Datenträger, komplette Partitionen oder Festplatten,

- unterstützte Löschverfahren: einfaches Überschreiben, Löschen nach BSI-Hinweisen, DoD 5220.22 oder Gutmann, Verwendung von Zufallszahlen, eigene Algorithmen,
- unterstützte Betriebs- und Dateisysteme: MS-DOS, Windows NT/2000/XP, Linux/Unix mit den jeweiligen Dateisystemen, Löschen fremder Dateisysteme (z.B. Löschen von Linux-Dateisystemen aus MS Windows heraus),
- Start von Bootmedium: Installation auf Festplatte erforderlich oder nicht,
- Erstellung eines Protokolls: Nachweis der Löschaktivitäten durch die Speicherung oder den Ausdruck eines Löschprotokolls,
- Benutzbarkeit: einfache Installation und Benutzung, Integration in die Arbeitsumgebung, Aufwand zur Schulung der Anwender,
- Performanz: erforderlicher Zeitaufwand für das Löschen.

Die Performanz wurde absichtlich an das Ende der Anforderungsliste gesetzt, da sie hier gegenüber der Sicherheit und Zuverlässigkeit zurückstehen sollte und ihre Bedeutung im Vergleich zu den anderen Kriterien deshalb deutlich geringer ist.

Der Vergleich von aktuell am Markt verfügbaren Löschwerkzeugen zeigt, dass das optimale Werkzeug, welches alle Anforderungen erfüllt, nicht existiert. Aus diesem Grund ist eine Entscheidung stets anhand der jeweils konkreten Situation, des Schutzbedarfs und der Art der zu löschenden Daten, der genutzten Systeme (Hardware, Betriebssystem und Anwendungssoftware), des Schulungsgrads der Benutzer sowie weiterer spezifischer Kriterien zu treffen.

Einen Überblick über einzelne Löschwerkzeuge, ihre Funktionen und ihre Leistungsfähigkeit findet man z.B. in [9], [12] und [10]. Die Kosten liegen jeweils zwischen dem Selbstkostenpreis (freie Software, Download aus dem Internet) und 1700 $ (DataScrubber). Im Folgenden werden Werkzeuge für die Betriebssysteme Windows und Linux vorgestellt, die viele der oben genannten Anforderungen erfüllen und frei verfügbar oder kostengünstig zu beschaffen sind.

5.2 Werkzeuge für MS Windows NT/2000/XP

Eraser (Heidi Computers Ltd.)
Das Löschwerkzeug Eraser ist frei unter der URL http://www.heidi.ie/eraser/ erhältlich. Der Quelltext steht unter der GNU Public License (GPL). Die aktuelle Version ist 5.7. Abbildung 1 zeigt exemplarisch die Benutzerschnittstelle.

Eraser gestattet das sichere Löschen unter MS Windows-Betriebssystemen (von Windows 95 bis XP). Es kann auf FAT- und NTFS-Dateisystemen einzelne Dateien und Verzeichnisse (auch wenn sie komprimiert oder verschlüsselt sind), den ungenutzten Speicherplatz auf einer Festplatte, die Auslagerungsdatei, temporäre Dateien, den Internet Cache und Cookies löschen. Hierzu werden die Löschverfahren nach DoD 5220.22-M, Gutmann (default) oder das Überschreiben mit Zufallszahlen verwendet. Besonderheiten sind die Integration in das Kontextmenü des Windows Explorer bzw. des Papierkorbs und das zeitgesteuerte Löschen durch nutzerdefinierte Tasks (s. Abbildung). Für das Löschen kompletter Festplatten oder Partitionen kommt das separate Programm DBAN (Darik's Boot and Nuke) zum Einsatz, dass auch von einer bootbaren Diskette gestartet werden kann.

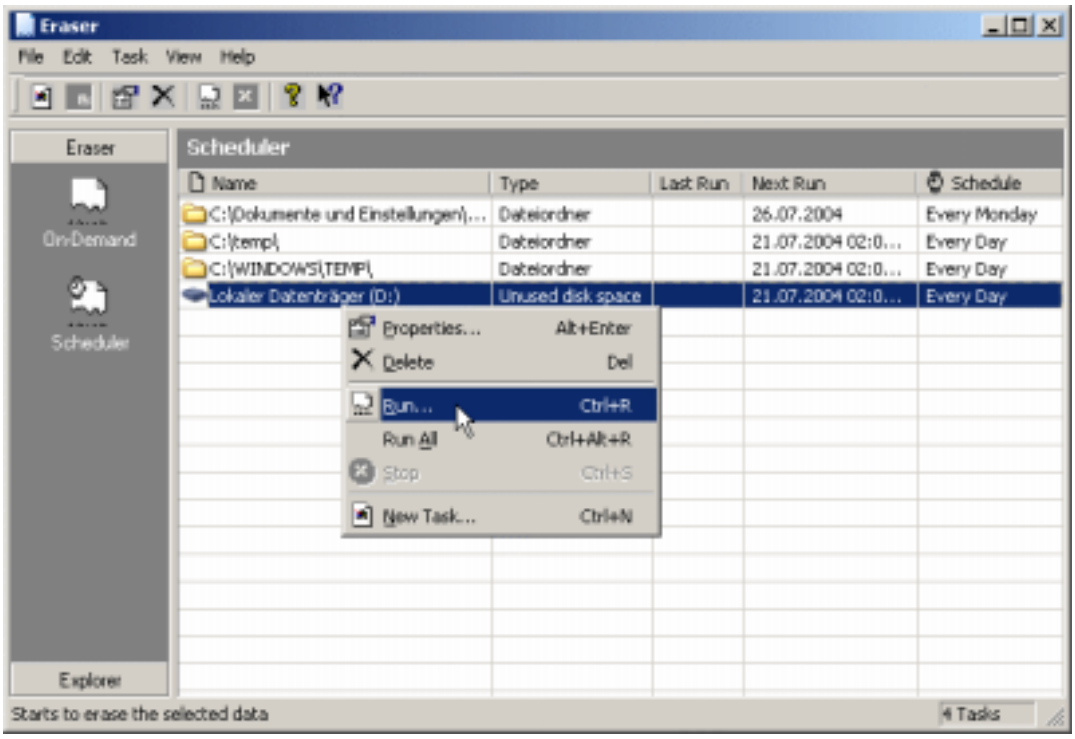

Abbildung 1: Benutzerschnittstelle von Eraser

Eraser kann keine Dateien oder Verzeichnisse in Dateisystemen löschen, die von Windows nicht erkannt werden. Dies trifft z.B. auf die gängigen Linux-Dateisysteme zu. Ein Löschprotokoll wird nicht erstellt.

5.3 Werkzeuge für Linux/Unix

Wipe
Wipe ist ein frei verfügbares Löschprogramm. Sein Quelltext steht unter der GNU Public License (GPL) und kann über die URL http://wipe.sourceforge.net/ geladen werden. Die aktuelle Version ist 2.2.0. Manche Linux-Distributionen (z.B. Suse Professional 9.1) enthalten Wipe schon, ansonsten sind Übersetzung und Installation des Programms unkompliziert. Bei der Bedienung von Wipe muss der Nutzer auf eine fensterorientierte Oberfläche verzichten – das Programm nutzt die Kommandozeile. Dafür passt es wegen seiner Größe auf eine Linux-Bootdiskette.

Wipe kann sowohl einzelne Dateien und Verzeichnisse als auch (etwas trickreich) komplette Partitionen und Festplatten löschen. Über Parameter beim Programmaufruf lässt sich das Verhalten steuern. Insbesondere kann das Löschverfahren beeinflusst werden. Die Möglichkeiten reichen vom einfachen oder mehrfachen Überschreiben mit dem konstanten Wert 0 oder einem benutzerbestimmbaren Wert über beliebig viele Zyklen mit Zufallszahlen bis hin zum Gutmann-Algorithmus. Nachfolgend sind die verwendbaren Parameter gezeigt (Kommandozeilenhilfe).

```
user@host:~> wipe -h
Wipe v2.2.0 - released January 10, 2004
by Tom Vier <nester@users.sf.net>

Usage is wipe [options] [file-list]

Options:         Default: wipe -ZdntVAkO -S512 -C4096 -l1 -x8 -p1
```

```
-h          --   help - display this screen
-u          --   usage
-c          --   show copyright and license
-w          --   show warranty information
-i  and  -I --   enable (-i) or disable (-I) interaction - overrides force
-f          --   force file wiping and override interaction
-r  and  -R --   recursion - traverse subdirectories
-s          --   silent - disable percentage and error reporting
-v          --   force verbose - always show percentage
-V          --   verbose - show percentage if file is >= 25K
-d  and  -D --   delete (-d) or keep (-D) after wiping
-n  and  -N --   delete (-n) or skip (-N) special files
-k  and  -K --   lock (-k) or don't lock (-K) files
-z          --   zero-out file - single pass of zeroes
-Z          --   perform normal wipe passes
-t  and  -T --   enable (-t) or disable (-T) static passes
-a  and  -A --   write until out of space (-a) or don't (-A)
-o[size] -O --   write to stdout (-o) or use files (-O)
-B(count)   --   block device sector count
-S(size)    --   block device sector size - default 512 bytes
                 or stdout write length when used with -A
-C(size)    --   chunk size - maximum file buffer size in kilobytes (2^10)
-l[0-2]     --   sets wipe secure level
-x[1-32] -X --   sets number of random passes per wipe or disables
-p(1-32)    --   wipe file x number of times
-b(0-255)   --   overwrite file with this value byte
```

Durch die Orientierung von Wipe auf die Kommandozeile lässt sich das Werkzeug gut für automatisierte Löschaktionen innerhalb ausführbarer Skripte verwenden.

Hinweis: Auch die bekannte Linux-Distribution Knoppix enthält auf der Live-CD ein Löschprogramm namens wipe. Dieses Programm ist ebenfalls kommandozeilenorientiert, stammt jedoch von einem anderen Autor und hat geringere Konfigurationsmöglichkeiten.

dd

dd ist ein universelles Standardwerkzeug, das in jeder Linux/Unix-Umgebung verfügbar ist. Es schreibt Daten von einer Eingabedatei in eine Ausgabedatei, evtl. mit zusätzlichen Konvertierungen. Die beteiligten Dateien können Unix-typisch auch Gerätedateien sein. So lässt sich als Eingabedatei z.B. /dev/zero oder /dev/random verwenden. Mit diesen Dateien steht ein quasi unerschöpflicher Strom von Zeichen mit dem ASCII-Wert 0 bzw. von Zufallszahlen zur Verfügung. Dieser Strom kann in die Gerätedatei einer Festplatte bzw. Partition (z.B. /dev/hda bzw. /dev/hda2) geschrieben werden, wobei der dort zuvor vorhandene Dateninhalt verloren geht. Das folgende Kommando überschreibt beispielsweise die zweite Partition der ersten IDE-Festplatte mit Zufallszahlen. Zusätzliche Parameter für die Blockgröße und Blockanzahl können angegeben werden:

```
user@host:~> dd if=/dev/random of=/dev/hda2
```

Das Überschreiben einzelner Dateien mit dd schlägt im Allgemeinen fehl, da nicht garantiert werden kann, dass die Daten in den Originalblöcken der Datei überschrieben werden.

Linux/Unix-Werkzeuge können in der Regel auch genutzt werden, um Partitionen bzw. Festplatten, die ein Windows-Dateisystem enthalten, komplett zu überschreiben.

6 Literatur

[1] Bremer, L.; Vahldiek, A.: Auf Nimmerwiedersehen – Dateien richtig löschen. c't 05/2003, S. 192-193.

[2] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch. verfügbar unter http://www.bsi.de/gshb/index.htm, 2003.

[3] Bundesamt für Sicherheit in der Informationstechnik: Wiederaufbereiten von VS-Datenträgern. Hinweisblatt Nr. 11 zur Umsetzung von § 12 der VS IT-Richtlinien des Bundesministerium des Innern. 21.11.1999.

[4] Camphausen, I.; Kelm, St.: Auferstanden. Verwchlüsselungssoftware PGP in neuen Versionen. iX 02/2003, S. 48-52.

[5] Dassow, P.: Verschlüsseln aber richtig. Fallstricke des Encrypted File System von Windows vermeiden. c't 12/2003, S.218.

[6] Department of Defense: National Industrial Security Program Operating Manual (NISPOM), verfügbar unter http://www.dss.mil/isec/nispom.htm, 1995.

[7] Department of Defense: Trusted Computer System Evaluation Criteria. DoD 5200.28-STD, 1985.

[8] Eckert, C.: IT-Sicherheit. Konzepte – Verfahren – Protokolle. Oldenbourg-Verlag, 2003.

[9] Garfinkel, S.L.; Shelat, A.: Remembrance of Data Passed: A Study of Disk Sanitization Practices. IEEE Security & Privacy, January/February 2003, S. 17-27.

[10] Großkreutz, M.: Porentief rein. Computerbild 13/2003, S.56-61.

[11] Grunwald, L.: Ausgrabungen – Beweissicherung bei Computerdelikten. iX 10/2002, S. 100-105.

[12] Grunwald, L.: Blitzblank – Sicheres Löschen von Speichermedien. iX 05/2003, S. 72-78.

[13] Gutmann, P.: Secure Deletion of Data from Magnetic and Solid-State Memory. 6th Usenix Security Symposium, verfügbar unter http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html, 1996.

[14] ITSEC – Information Technology Security Evaluation Criteria. Harmonised Criteria of France, Germany, the Netherlands, the United Kingdom (Version 1), 1990.

[15] IT-Sicherheitskriterien – Kriterien für die Bewertung der Sicherheit in der Informationstechnik (1. Fassung). Bundesanzeiger, Köln 1989.

[16] Kersten, H.: Sicherheit in der Informationstechnik, Einführung in Probleme, Konzepte und Lösungen. Oldenbourg-Verlag, 1995.

[17] Morgenstern, H.: Digitale Autopsie – Computer-Forensik mit Open Source Tools. c't 07/2004, S. 200-203.

[18] National Institute of Standards and Technology: Common Criteria for IT Security Evaluation (Version 2.1), verfügbar unter http://csrc.nist.gov/cc/index.html, 1999.

[19] Pfitzner, R.: Sicheres Löschen von Dateien – Standards, Löschtools, Empfehlungen. Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg, Internes Arbeitspapier, 2003.

[20] Rabanus, C.: Die Profis – Datenrettung in Speziallaboren. c't, 06/2000, S. 130-137.

[21] Tennert, O.: Sesam, schließe dich. Verschlüsselte Dateisysteme unter Linux. iX 11/2002, S. 58-66.

[22] The Register Online News: Oops! Firm accidentally eBays customer database. verfügbar unter http://www.theregister.co.uk/2004/06/07/hdd_wipe_shortcomings/, 07.06.2004.