Dirk Fox

Sicheres Löschen von Daten auf Festplatten

Über die richtige Methode zum logischen Löschen von Daten auf Festplatten, die einem anderen Zweck zugeführt, wiederverwendet oder verkauft werden sollen, wird immer wieder kontrovers diskutiert. Tatsächlich müssen Empfehlungen regelmäßig an die technische Entwicklung angepasst werden – und die erlaubt inzwischen einfachere Verfahren.

1 Hintergrund

Eine der häufigsten Ursachen für den unkontrollierten Abfluss von Daten aus Unternehmen und Behörden ist die Entsorgung von Papier und Speichermedien. Die Liste der bekannt gewordenen Fälle reicht von Patientenakten in Müllcontainern bis zu Entwicklungsdaten eines Automobilkonzerns auf der Festplatte eines ersteigerten Gebrauchtcomputers.

Für die sichere Vernichtung von Papierdokumenten gibt es seit langem einen Standard – die DIN 32757-1 vom Januar 1995, in der fünf Sicherheitsstufen definiert werden (siehe Tabelle). Für personenbezogene Daten wird häufig die Vernichtung nach Sicherheitsstufe 3, für besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG, wie Patientendaten) Sicherheitsstufe 4 gefordert (siehe z. B. [1]).

Tabelle | Sicherheitsstufen für Papier-Schredder gemäß DIN 32757

	Anforderung	Dokumentenklasse
1	B: ≤ 12 mm	Allgemein
2	B: ≤ 6 mm	Intern
3	B: ≤ 4 mm, L: ≤ 8 cm	Vertraulich, personenbezogen
4	B: ≤ 2 mm, L: ≤ 1,5 cm	Geheim, besondere Arten personenbez. Daten
5	B: ≤ 0,8 mm, L: ≤ 1,3 cm	Streng geheim

Dirk Fox

Geschäftsführer der Secorvo Security Consulting GmbH und Herausgeber der DuD.
E-Mail: dirk.fox@secorvo.de

Sollen Speichermedien mit digitalen Daten sicher entsorgt werden, kann dies durch mechanische (Zerstörung) oder thermische Verfahren (Erhitzung) erfolgen. Die unterschiedlichen Entsorgungsverfahren eignen sich je nach Speichermedium unterschiedlich gut.

So lassen sich CDs und DVDs heute mit geeigneten Schreddern wirksam mechanisch zerstören. Zumindest für Daten der Dokumentenklassen „intern“ und „vertraulich“ sollte dies ausreichen. Will man ganz sicher gehen, dass eine Rekonstruktion technisch unmöglich ist, sollte man geeignete thermische Entsorgungsverfahren wählen.

Bei kleineren Mengen magnetischer Speichermedien (Festplatte, Magnetbänder) kann der Aufwand für eine wirksame mechanische Zerstörung, die auch das magnetische Material vernichtet, zu hoch sein. Auch eine thermische Entsorgung magnetischer Medien ist meist nur bei großen Mengen vertretbar, da für die Entmagnetisierung sehr hohe Temperaturen erforderlich sind. Durchgesetzt haben sich daher für magnetische Medien so genannte „Degausser“, die das Medium einem starken, wechselnden Magnetfeld aussetzen und so gespeicherte Daten löschen. In DIN 33858 sind Anforderungen an solche Degausser spezifiziert.

Alle angeführten Entsorgungsverfahren haben bei digitalen Datenspeichern jedoch eine Vernichtung des Mediums zur Folge: Es kann anschließend nicht mehr zur Speicherung von Daten genutzt werden. Bei Festplatten ist genau das aber häufig nicht erwünscht: Soll ein ausgemusterter Rechner für andere Zwecke eingesetzt, verkauft oder vom Leasing-Unternehmen zurückgenommen werden, ist eine funktionserhaltende Beseitigung der auf der Festplatte gespeicherten Daten erforderlich, will man das Auswechseln und die Entsorgung des Festplattenspeichers vermeiden. Wie aber lassen sich auf Festplatten gespeicherte Daten nicht rekonstruierbar löschen?

2 Löschen auf Festplatten

Aus mehreren Gründen stellt das irreversible logische Löschen von Daten auf Festplatten eine Herausforderung dar.

2.1 Betriebssystem

Werden Daten mit dem Lösch-Befehl gängiger Betriebssysteme beseitigt, so lassen sie sich bei den meisten Betriebssystemen leicht wieder rekonstruieren. Denn dabei wird eine gelöschte Datei lediglich in einen virtuellen „Papierkorb“ verschoben – und dabei nur der Verzeichniseintrag entfernt. Zugleich werden Dateiname und alle Angaben zum ursprünglichen Speicherort in einem versteckten Verzeichnis („Recycler“) abgelegt, wo sie über den „Papierkorb“ weiter zugänglich sind. Die Inhalte der Datei bleiben erhalten und sind vor Überschreiben geschützt, so lange die „gelöschte“ Datei noch über den „Papierkorb“ zugänglich ist und per Mausklick wiederhergestellt werden kann.

Wird die Datei schließlich durch ein „Leeren“ des Papierkorbs beseitigt (oder unter Windows bei gleichzeitig gedrückter Shift-Taste gelöscht), verschwindet der Eintrag im Papierkorb. Davon sind der Dateiname und alle Verzeichniseinträge betroffen. Der Inhalt der Datei ist jedoch weiterhin vorhanden, nun aber vom Be-

triebssystem zum Überschreiben mit anderen Daten freigegeben. Bis dahin besteht jedoch zumindest grundsätzlich die Möglichkeit, auch eine gelöschte Datei zu rekonstruieren. Das kann mühsam sein, da die Inhalte auf weit auseinander liegende Sektoren der Festplatte verteilt sein können und der Verzeichniseintrag, der die von der Datei belegten Sektoren der Festplatte und deren Reihenfolge angibt, nicht mehr existiert.

Erst wenn die von einer gelöschten Datei belegten Sektoren mit neuen Daten überschrieben werden, ist eine Rekonstruktion mit einfachen forensischen Software-Tools nicht mehr möglich. Mit der zunehmenden Größe von Festplatten kommt das Überschreiben einer alten Datei jedoch immer seltener vor; meist führt erst eine Defragmentierung („Aufräumen") des Datenträgers zum Überschreiben von Sektoren gelöschter Dateien.

2.2 Speichertechnik

Digitale Daten werden auf magnetischen Datenträgern durch eine elektromagnetische „Polarisierung" des magnetisierbaren Materials gespeichert. Aufgrund mechanischer Toleranzen der Schreib-Leseköpfe kommt es dabei unvermeidlich zu geringen Abweichungen von einer „idealen" Speicherung (unsauberer Signalverlauf, seitliche Abweichungen von der „Spur"). Anders als bei analogen Daten führen diese Abweichungen aber in der Regel nicht zu Lesefehlern, da das vom Lesekopf eingelesene Signal lediglich eindeutig als „0"- oder „1"-Folge interpretiert werden muss, Abweichungen also durch „Auf-" oder „Abrunden" korrigiert werden. Die Speicherverfahren unterstützen die Unterscheidung, indem sie spezielle Kodierungen für bestimmte Bitfolgen verwenden, wie beispielsweise Run Length Limited (RLL) oder Modified Frequency Modulation (MFM).

Bei einigen älteren Speichertechniken für Festplatten führten die mechanischen Schreibkopftoleranzen dazu, dass beim Überschreiben von Bereichen einer Festplatte mit neuen Daten Reste der Magnetisierungen der zuvor dort gespeicherten Daten erhalten blieben. Analysierte man die vom Lesekopf aufgenommenen (analogen) Werte später mit einem Oszilloskop, konnten aus den Abweichungen von einem „idealen" Verlauf des Signalpegels die Werte der zuvor dort gespeicherten Bits abgeleitet werden.

Heutige Speichertechniken schreiben Daten mit erheblich höherer Dichte auf Magnetdatenträger. Sie arbeiten nicht mehr mit „Peak"-Signalen, sondern mit „analogen Mustern" für Bitfolgen, die sie über Näherungsalgorithmen interpretieren, wie beispielsweise Extended Partial Response/Maximum Likelihood (EPRML). Ein „Herausfiltern" überschriebener Daten anhand des analogen Signals mit Hilfe eines Oszilloskops ist daher heute nicht mehr möglich. Dennoch können auch bei EPRML nach dem Überschreiben Restinformationen auf dem Speichermedium verbleiben, die sich allerdings wegen der hohen Speicherdichte heutiger Speichertechniken nur sehr aufwändig zurückgewinnen lassen.

3 Gängige Empfehlungen

Anders als bei der Vernichtung von Papierdokumenten gibt es für das sichere „logische" Löschen von Daten auf Festplatten keinen einheitlichen Standard, sondern nur sehr unterschiedliche Empfehlungen.

Einige der noch vor einigen Jahren empfohlenen Techniken, wie z. B. die „low-level"-Formatierung der Festplatte, werden von heutigen Betriebssystemen nicht mehr unterstützt. So sorgt das Format-Kommando von Windows nur für eine Freigabe aller Sektoren, überschreibt alte Daten auf dem Medium jedoch nicht.

3.1 Gutmann-Empfehlung

Im Jahr 1996 veröffentlichte Peter Gutmann eine Untersuchung über Möglichkeiten zur Verhinderung der Wiedergewinnung gelöschter Daten auf Festplatten [2]. Seiner Betrachtung lag eine Analyse der damals eingesetzten Bitfolgen-Kodierungen für Plattenspeicher zu Grunde, insbesondere MFM und RLL.

Um eine Wiedergewinnung einzelner überschriebener Bits zu verhindern, empfahl Gutmann ein Überschreiben mit einer Folge spezifischer Bitmuster, die auf die unterschiedlichen Bitfolgen-Kodierungen von (1,7) RLL, (2,7) RLL und MFM zugeschnitten waren. Mit jeweils vier Überschreibzyklen mit Zufallsfolgen zu Beginn und zum Schluss summierten sich die Durchläufe – abhängig vom Schreibverfahren – auf 18 bis 26; und nicht, wie häufig publiziert, auf 35.

Für neuere Speichertechniken wie das damals aufkommende PRML sowie die Weiterentwicklung EPRML, durch die eine Rückgewinnung überschriebener Daten erheblich erschwert wird, ist seine Empfehlung einfach: „A good scrubbing with random data will do about as well as can be expected".

3.2 DoD 5220.22-M

Gerne und häufig wird die Direktive DoD 5220.22-M („National Industrial Security Program – Operating Manual", NISPOM) des US-amerikanischen Verteidigungsministeriums vom Januar 1995 zitiert, nach der zum logischen Löschen auf magnetischen Speichermedien ein dreimaliges Überschreiben (zuerst mit einem beliebigen festen Wert, dann mit dem binären Komplement dieses Wertes und schließlich mit Zufallsfolgen) und für besonders sensible Daten ein siebenmaliges Überschreiben (zweimal obige Prozedur, dazwischen ein weiteres Überschreiben mit Zufallswerten) gefordert wird. Tatsächlich wurde die Direktive inzwischen – zuletzt am 28.02.2006 – durch eine Neufassung ersetzt, in der sich kein Hinweis mehr auf diese Löschmethode findet [3].

In der in diesem Zusammenhang gerne zitierten Special Publication SP 800-88 "Guidelines for Media Sanitization" vom September 2006 weist das US-amerikanische NIST darauf hin, dass „studies have shown that most of today's media can be effectively cleared and purged by one overwrite using current available sanitization technologies." [4]

3.3 IT-Grundschutz

In den IT-Grundschutz-Maßnahmenkatalogen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) werden, in Anlehnung an die DoD-Direktive, in M 2.167 „Sicheres Löschen von Datenträgern" zwei bis drei Überschreibzyklen (fester Wert, Komplement, Zufallsfolge) empfohlen [5].

Vor allem aber wird darauf hingewiesen, dass das Löschen einer Datei meist nicht ausreicht, da sich auf einem System zahlreiche Kopien der Datei befinden können – z. B. temporäre oder Backup-Dateien, Cache-Inhalte oder Auslagerungsdateien wie Swap-Files oder Hibernation-Files. Meistens liegen die Kopien unter anderem Namen in anderen Verzeichnissen

und sind daher oft nur mit manuellem Aufwand zu finden und zu beseitigen.

3.4 Datenschutz-Empfehlungen

Im IT-Grundschutz-Baustein B 1.5 „Datenschutz" werden in der Maßnahmenempfehlung M 7.15 „Datenschutzgerechte Löschung/Vernichtung" für das Löschen von personenbezogenen Daten mindestens sieben, bei Daten hoher Schutzstufe sogar mindestens 33 Überschreibzyklen gefordert [6].

Diese Forderung findet sich bereits in der Orientierungshilfe „Sicheres Löschen magnetischer Datenträger" des AK Technik der Datenschutzbeauftragten aus dem Jahr 2004 [7] und geht auf Überlegungen von Roy Pfitzner zurück, nach denen beim Überschreiben mit Zufallswerten spätestens nach 33 Zyklen jedes Bit mit hoher Wahrscheinlichkeit mindestens einmal invertiert worden ist [8].

3.5 Bewertung

Alle angeführten Empfehlungen orientieren sich an der Zielsetzung, die Wiedergewinnung auch nur eines einzigen Bits müsse wirksam verhindert werden. Tatsächlich genügt es jedoch in der Praxis bei weitem, die korrekte Rekonstruktion einer ganzen Datei hinreichend unwahrscheinlich zu machen.

Craig Wright, Dave Kleiman und Shyaam Sundhar wiesen im Dezember 2008 in einem Beitrag auf der Konferenz ICISS 2008 zu Recht darauf hin, dass vor allem bei modernen Schreibverfahren wie EPRML die Rekonstruktion eines einzigen, einmal überschriebenen Bits immer nur mit einer gewissen Wahrscheinlichkeit gelingt [9].

Damit sinkt die Aussicht, eine ganze Datei selbst nach einmaligem Überschreiben noch rekonstruieren zu können, auf eine vernachlässigbare Größe, wie eine einfache Rechnung zeigt:

- **Selbst wenn die Erfolgsaussicht für die Rekonstruktion eines einzigen Bits unrealistische 99,9 % erreicht, liegt die Wahrscheinlichkeit, auch nur jedes zehnte Byte einer 20 kB großen Datei korrekt zu rekonstruieren, bei 0,000076 % – das entspricht der Chance auf einen 6er im Lotto.**

4 Empfehlungen

Angesichts der hohen Datendichte heutiger magnetischer Datenträger und Schreib-/Leseverfahren, die gespeicherte Bitfolgen über Wahrscheinlichkeiten und fehlerkorrigierende Codes zurückgewinnen, ist eine erfolgreiche Rekonstruktion überschriebener Daten vernachlässigbar unwahrscheinlich. Daher genügt auf modernen Festplatten in der Praxis ein einmaliges Überschreiben mit Zufallswerten für ein sicheres Löschen vollauf.

Tatsächlich ist es erheblich wichtiger, eine vollständige Löschung sicher zu stellen, als mehrere Überschreibzyklen zu fordern.

4.1 Beseitigung von Restinformationen

Ein Löschvorgang sollte nicht nur die diversen Kopien einer Datei (siehe die Hinweise unter 3.3) umfassen, sondern auch die Bereinigung des so genannten „Slack-Space". Darunter wird der ungenutzte Bereich in der letzten „Zuordnungseinheit" einer Datei auf dem Speichermedium verstanden. Die Größe einer Zuordnungseinheit – der kleinsten auf dem Medium adressierbaren Speichermenge – hängt von dem genutzten Dateisystem und der Gesamtgröße der Partition ab, in der eine Datei gespeichert wird und liegt zwischen 4 kB (NTFS) und bis zu 64 kB (FAT32).

Da die Größe einer Datei in der Regel nicht einem Vielfachen der Größe einer Zuordnungseinheit entspricht, bleibt in der letzten Zuordnungseinheit hinter dem „offiziellen Dateiende" ungenutzter Speicher übrig. In diesem Bereich können jedoch Daten gespeichert sein – seien es verbliebene Daten einer vorausgegangenen Nutzung, Inhalte des Festplatten-Cache oder Daten aus dem RAM-Speicher des PC, die mit dem letzten Block der Datei auf die Festplatte geschrieben wurden.

Das BSI weist in seinem Maßnahmenkatalog zum IT-Grundschutz in M 4.64 („Beseitigung von Restinformation") auf dieses Problem hin und empfiehlt die Löschung insbesondere dieser Bereiche vor der Weitergabe einer Festplatte [11].

4.2 Tools

Inzwischen sind zahlreiche Tools zum wirksamen Löschen von auf Festplatten gespeicherten Daten verfügbar.[1] Einige ausgewählte verbreitete Tools werden im Folgenden kurz vorgestellt.

Betriebssystem-Bordmittel
Microsoft liefert seit Windows 2000 ein wenig bekanntes, aber mächtiges Kommandozeilen-Tool namens `cipher.exe` mit. Es dient in erster Linie dazu, die Windows-eigene Verschlüsselung EFS (Encrypted File System) zu administrieren. Mit der Option `cipher /w: <Vol>` stellt es jedoch eine leistungsfähige Löschfunktion bereit, die das ausgewählte Volume von allen bereits gelöschten und allen temporären, nicht mehr benötigten Dateien (wie in DoD 5220.22-M von 1995 empfohlen) durch dreimaliges Überschreiben mit #0, #F und Zufallswerten befreit.

In das Betriebssystem MAC OS X ist eine Löschfunktion integriert, die ein mehrfaches Überschreiben des Dateiinhalts bewirkt. Sie ist über den Finder mit der Option „Papierkorb sicher entleeren" erreichbar. Ab Version 10.2.3 ist ein Löschen aller Dateien einer Festplatte durch Überschreiben über das „Festplatten-Dienstprogramm" möglich. Dazu muss der MAC zuvor von CD gebootet worden sein.

Unter Linux hilft das Data Dump-Kommando (dd), mit dem vorgegebene oder zufällige Daten auf ein Speichermedium geschrieben werden können. Eine Löschung nach Gutmann bieten die Open Source Lösungen wipe[2] (v2.2.0) und shred[3] (v1.5.9), mit denen einzelne Dateien inklusive Slack-Space in 25-35 Zyklen überschrieben werden.

Eraser[4]
Das freie Open-Source-Tool Eraser (v5.86a) der irländischen Firma Heidi Computers Ltd. stellt ein komfortables Lösch-Tool für Windows-Betriebssysteme dar. Über die rechte Maustaste erreichbar, erlaubt es ein sicheres Verschieben und Löschen von Dateien nach verschiedenen voreinstellbaren Verfahren. So werden das Schema von Peter Gutmann (mit allen 35 Überschreibzyklen), die US-DoD-Empfehlung 5220.22-M von 1995 (drei- bzw. siebenmaliges Überschreiben), das Überschreiben mit Zufallsfolgen sowie das von

1 Siehe z. B. die Übersicht in http://archive.dban.org/mirrors/www.rcmp.gc.ca/tsb/pubs/it_sec/b2-001_e.pdf.
2 Download: http://wipe.sourceforge.net/
3 Download: http://srm.sourceforge.net/
4 Download: Heidi Computers Ltd., http://www.heidi.ie/node/6 .

Bruce Schneier 1996 empfohlene Überschreiben in sieben Zyklen („1“, „0“, fünf Mal mit Zufallsfolgen [10]) unterstützt.

In den Löschprozess eingeschlossen sind auch die Slack-Spaces der letzten Zuordnungseinheiten einer Datei sowie alle betroffenen Verzeichniseinträge.

DBAN[5]
Das Open Source Tool „Darik's Boot And Nuke“ (v2.0.0 vom 21.02.2008) umfasst eine vollständige Boot-Disk und erlaubt das “Wipen” von kompletten Festplatten nach den beiden vom DoD empfohlenen Verfahren, der Empfehlung von Peter Gutmann und ein einmaliges Überschreiben mit einer Zufallsfolge. Es eignet sich insbesondere für Administratoren, die PC-Systeme für die Rückgabe oder Wiederverwendung bereinigen müssen.

VS-Clean[6]
Für Behörden hat das BSI das Programm VS-Clean (v2.1) entwickelt, das von Bundes-, Landes- und Kommunalverwaltungen über die Webseiten des BSI kostenlos bestellt werden kann. VS-Clean erlaubt die unwiderrufliche Löschung von AT/(E) IDE/SCSI-Festplatten bis zur Geheimhaltungsstufe „VS-Vertraulich“ durch mehrmaliges Überschreiben mit wechselnden Bitmustern.

4.3 Verschlüsselung

Eine wirksame Maßnahme ist auch die Verschlüsselung der auf dem System gespeicherten Daten. Sofern das Passwort gut gewählt ist, das Verschlüsselungsprogramm keine Hintertür besitzt, ein ausreichend sicheres Verschlüsselungsverfahren (wie beispielsweise der AES) gewählt wird und der Verschlüsselungsschlüssel eine Länge von mindestens 128 bit besitzt, kann man sich bei der Bereinigung des Datenträgers getrost auf ein einfaches Löschen der Datei beschränken.

Aber Vorsicht: Werden nur einzelne Dateien, Verzeichnisse oder Volumes verschlüsselt („Container-Verschlüsselung“), kann nicht ausgeschlossen werden, dass vollständige oder Teilkopien der verschlüsselten Daten unverschlüsselt in temporären Verzeichnissen oder Auslagerungsdateien liegen. So werden von einer Container-Verschlüsselung in der Regel Spuren wie temporäre Dateien (z. B. zwischengespeicherte Arbeitsergebnisse, Inhalte angeklickter E-Mail-Anhänge, Dateien geöffneter Zip-Container etc.), die URLs und die Inhalte der zuletzt besuchten Webseiten oder die Liste der zuletzt geöffneten Dokumente nicht erfasst.

Daher ist eine Vollverschlüsselung des gesamten Systems zu empfehlen, will man aufwändige Überschreib-Prozeduren bei einer späteren Bereinigung des Datenträgers vermeiden.

4.4 Organisatorische Prozesse

Nicht zuletzt erfordert ein wirksamer Schutz vor unkontrolliertem Datenabfluss über (magnetische) Speichermedien organisatorische Disziplin. Aus sehr unterschiedlichem Anlass können Festplatten eine Organisation verlassen:

- bei einer Reparatur durch den Hersteller,
- beim Austausch in der Garantiezeit,
- bei der Rückgabe des Geräts an den Leasingpartner,
- beim Verkauf als Gebrauchtgerät und schließlich
- bei der Ausmusterung als Elektronikschrott.

Bei allen diesen Prozessen muss sichergestellt werden, dass sensible und personenbezogene Daten zuvor gelöscht oder, wenn das nicht möglich ist, der Dienstleister auf das Datengeheimnis verpflichtet und die korrekte Rückgabe der Festplatte sichergestellt wird.

Dabei sind nicht nur Computer-Festplatten zu berücksichtigen, sondern ebenso alle Speichereinheiten in Peripheriegeräten wie z. B. größeren Druckern und Kopiergeräten. Ist das Speichermedium defekt und kann es daher nicht durch Überschreiben gelöscht werden, ist eine mechanische oder thermische Vernichtung unvermeidlich.

5 Fazit

Auch wenn keine öffentlichen Untersuchungen dazu vorliegen, dürfte eine fehlerfreie Rekonstruktion überschriebener Dateien auf einer modernen Festplatte praktisch unmöglich sein – selbst bei einer sehr hohen Rekonstruktionswahrscheinlichkeit für ein einzelnes Bit. Ein einmaliges Überschreiben mit Zufallsfolgen sollte daher auch bei besonders sensiblen personenbezogenen Daten völlig ausreichen, sofern beim Überschreiben der gesamte Slack-Space (und alle Kopien) eingeschlossen wird. Defizite finden sich in der Praxis zumeist in organisatorischen Prozessen, die eine unkontrollierte Ausmusterung ungelöschter Datenträger nicht verhindern.

5 Download: http://www.dban.org/
6 Bezug: http://www.bsi.de/produkte/vsclean/

Literatur

[1] Der Landesbeauftragte für den Datenschutz Niedersachsen: *Vernichtung von Datenträgern mit personenbezogenen Daten*. 27.05.2002 http://cdl.niedersachsen.de/blob/images/C422235_L20.pdf (15.02.2009)

[2] Gutmann, Peter: Secure Deletion of Data from Magnetic and Solid-State Memory. Proceedings of 6th USENIX Security Symposium, San José, 22.-25.07.1996 http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html (15.02.2009)

[3] Department of Defense: *National Industrial Security Program – Operating Manual (NISPOM)*. DoD 5220.22-M vom 28.02.2006 https://www.dss.mil/GW/ShowBinary/DSS/isp/odaa/documents/nispom2006-5220.pdf (15.02.2009)

[4] National Institute of Standards and Technology (NIST): *Guidelines for Media Sanitization. NIST Recommendations*, Special Publication NIST SP 800-88 vom 11.09.2006 http://csrc.nist.gov/publications/nistpubs/800-88/NIST-SP800-88_rev1.pdf (15.02.2009)

[5] Bundesamt für Sicherheit in der Informationstechnik (BSI): *M 2.167 Sicheres Löschen von Datenträgern*. IT-Grundschutz-Kataloge, 10. Ergänzungslieferung 2008 http://www.bsi.de/gshb/deutsch/m/m02167.htm (15.02.2009)

[6] Bundesamt für Sicherheit in der Informationstechnik (BSI): *IT-Grundschutz-Baustein Datenschutz B 1.5* vom 04.07.2007 https://ssl.bsi.bund.de/gshb/baustein-datenschutz/dokumente/b01005.pdf (15.02.2009)

[7] AK Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder: *Orientierungshilfe Sicheres Löschen magnetischer Datenträger* vom 07.10.2004 http://www.hamburg.de/contentblob/254804/data/sicheres-loeschen.pdf (15.02.2009)

[8] Pfitzner, Roy: *Sicheres Löschen von Dateien – Standards, Löschtools, Empfehlungen*. Internes Arbeitspapier, LDSB Brandenburg, 2003.

[9] Wright, Craig; Kleiman, Dave; Sundhar, Shyaam: *Overwriting Hard Drive Data: The Great Wiping Controversy*. Zusammenfassung im SANS Forensic Blog vom 15.01.2009 http://sansforensics.wordpress.com/2009/01/15/overwriting-hard-drive-data/ (15.02.2009)

[10] Schneier, Bruce: *Applied Cryptography*, 2nd Edition, John Wiley & Sons, 1996.

[11] Bundesamt für Sicherheit in der Informationstechnik (BSI): *M 4.64 Verifizieren der zu übertragenen Daten vor Weitergabe / Beseitigung von Restinformationen*. IT-Grundschutz-Kataloge, 10. Ergänzungslieferung 2008 http://www.bsi.de/gshb/deutsch/m/m04064.htm (15.02.2009)