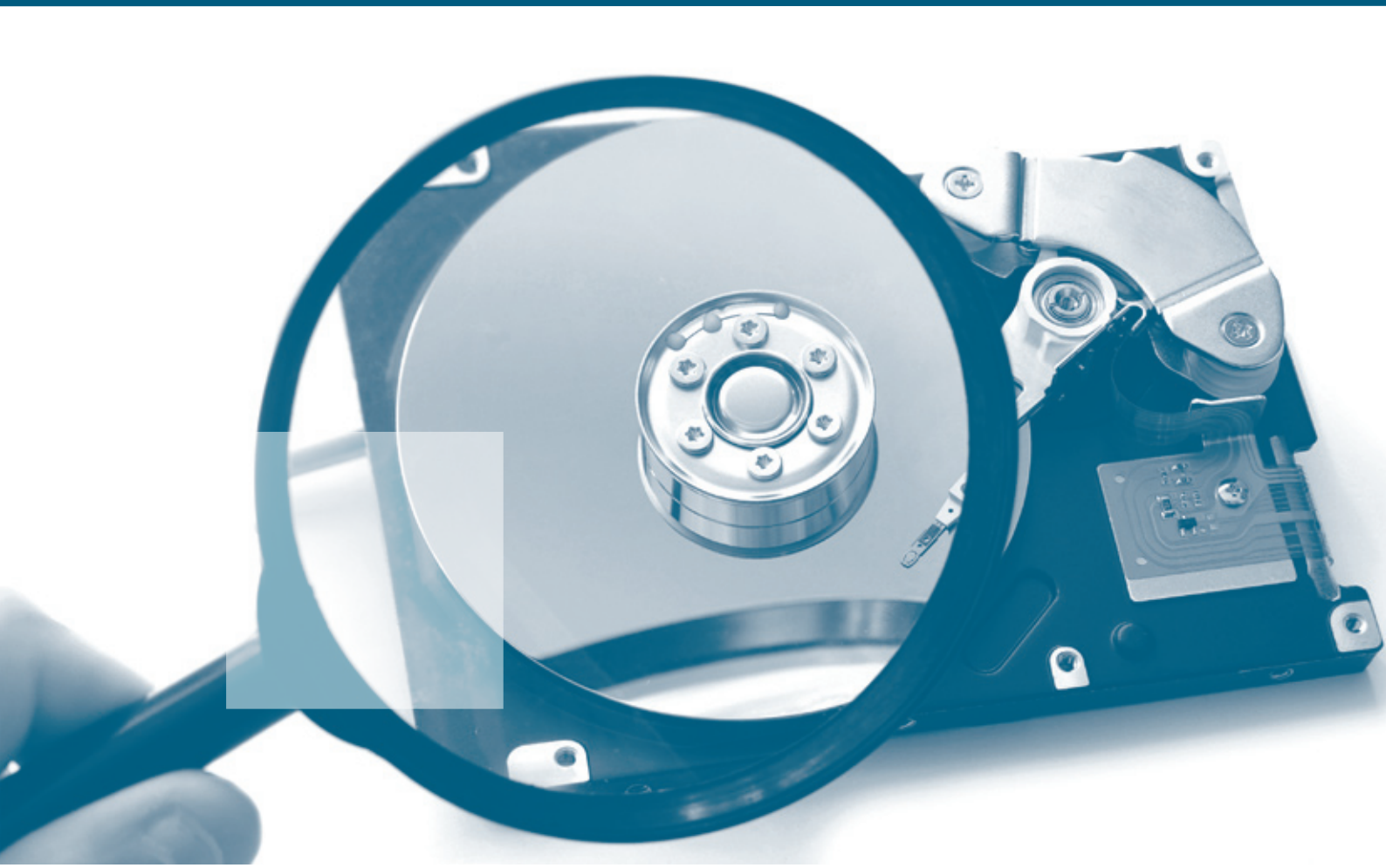

Leitfaden zum Sicheren Datenlöschen

Version 2.0

BITKOM

Impressum

Herausgeber:	BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. Albrechtstraße 10 A 10117 Berlin-Mitte Tel.: 030.27576-0 Fax: 030.27576-400 bitkom@bitkom.org www.bitkom.org
BITKOM-Gremium:	AK Speichertechnologien
Ansprechpartner:	Dr. Ralph Hintemann Tel.: 030.27576-250 r.hintemann@bitkom.org
Redaktion:	Dr. Ralph Hintemann, Christine Faßnacht (BITKOM)
Gestaltung / Layout:	Design Bureau kokliko / Anna Müller-Rosenberger (BITKOM)

Bildnachweis: Stockxpert

Leitfaden zum Sicheren Datenlöschen

Version 2.0

BITKOM

Inhaltsverzeichnis

1 Einleitung

Der Schutz von firmeninternen und privaten Daten vor unberechtigtem Zugriff nimmt eine zunehmend wichtigere Rolle in der Unternehmensführung ein. Es ist ein steigendes Bewusstsein zu verzeichnen, dass IT-Sicherheit ein wichtiges Instrument der Geschäftsleitung ist, um ihrer Verantwortung gegenüber dem Unternehmen, den Mitarbeitern, Kunden, Aktionären oder Anteilseignern gerecht zu werden. Auch Privatnutzer werden zunehmend sensibler in Hinsicht auf den möglichen unberechtigten Zugriff auf ihre Daten und setzen zum Beispiel private Firewalls ein.

Die Notwendigkeit, den unberechtigten Zugriff auf Unternehmensdaten von außen zu verhindern, ist allgemein anerkannt. Bei größeren IT-Systemen wird dafür ein hoher Aufwand betrieben. Das Bewusstsein, dass Daten nach einer unvollständigen Löschung auf nicht mehr benötigten Datenträgern nach außen gelangen können, ist im Gegensatz dazu noch kaum vorhanden. Hier sind kaum Verfahren entwickelt und Prozesse definiert, wie nach der Nutzung der Systeme mit den nicht mehr verwendeten Datenträgern umgegangen werden soll. So werden, meistens durch Unwissenheit, häufig erhebliche Sicherheitslücken zugelassen, über die Informationen unabsichtlich oder böswillig aus dem Unternehmen getragen werden können. Auf diese Weise können interne Betriebsdaten, sensible Kundeninformationen, Passwörter, Zugangsdaten oder andere persönliche Daten leicht in falsche Hände geraten. Nicht mehr benötigte Datenträger werden an Dritte weitergegeben, ohne dabei sicherzustellen, dass die darauf enthaltenen Informationen sicher gelöscht sind und auch nicht wieder hergestellt werden können. Eine ausreichende Sorgfalt der Unternehmen ist insbesondere auch aus (datenschutz-)rechtlichen Gründen und ggf. aus vertraglichen Verpflichtungen beim Umgang mit Kundendaten erforderlich. Im Falle eines Missbrauchs können beispielsweise Haftungsansprüche Geschädigter gegen die Geschäftsführung geltend gemacht werden. Die nachhaltige Datenlöschung nicht mehr benötigter Datenträger sollte in keinem IT Sicherheitskonzept fehlen.

Dass die gängige Praxis zurzeit anders aussieht, zeigen Untersuchungen, in denen gebrauchte Datenträger erworben und auf die Möglichkeit eines Zugangs zu den (ehemals) darauf gespeicherten Daten überprüft werden (z.B.: Garfinkel: Remembrance of Data Passed). So konnten in Untersuchungen ohne großen Aufwand z.B. auf sensible Patientendaten einer Krankenkasse oder Buchungsinformationen einer Bank zugegriffen werden. Es gibt viele Wege, über die Daten unbeabsichtigt schnell das Unternehmen verlassen: die Versteigerung gebrauchter Festplatten über Online-Auktionen (z.B. eBay) oder andere Kanäle, das Weitergeben von Hardware an firmeninterne Abteilungen, der Verkauf von ausrangierten Firmen-PCs an Mitarbeiter oder die bei Rückgabe von Leasinggeräten auf einem PC oder Kopierer gespeicherten Dokumente.

Mit diesem Informationspapier möchte BITKOM eine erste Hilfestellung geben, um Daten sicher zu löschen. Inhaltlicher Schwerpunkt bildet die Datenlöschung von Datenträgern, wie Fest- oder Wechselplatten, aber auch Bändern, Speicherkarten, WORM oder MO-Medien, da in diesem Zusammenhang mit Abstand die häufigsten Sicherheitsmängel auftreten.

2 Ansätze und Möglichkeiten der Datenlöschung

2.1 Überblick

Daten werden physikalisch auf einer Festplatte durch die Magnetisierung kleinster Eisenpartikel gespeichert, die entsprechend ihrer Ausrichtung den Wert 0 oder 1 darstellen. Die Daten werden in Sektoren zusammengefasst, eine Datei besteht aus einem oder mehreren Sektoren. Der Dateiname und die Angaben über den Speicherort werden in dem Inhaltsverzeichnis des Datenträgers (z.B. der „MFT“ – Master-File-Table) abgelegt (vergleichbar mit dem Inhaltsverzeichnis eines Buches).

Die gespeicherten Daten, d.h. die magnetischen Information werden nur durch Überschreiben der entsprechenden Bereiche mit anderen Daten verändert.

Selbst überschriebene Datenbereiche lassen sich teilweise – allerdings nur in speziellen Laboren – wieder rekonstruieren. Das liegt daran, dass bei der Änderung der Magnetisierung niemals alle Eisenpartikel ummagnetisiert werden. Durch mehrfaches Überschreiben der Datenbereichen mit unterschiedlichen Daten (Bit-Mustern) können die ursprünglichen Informationen aber nachhaltig gelöscht werden.

Wie oft ein Datenträger dabei überschrieben werden muss, hängt von der verwendeten Speichertechnologie (je höher die Aufzeichnungsdichte, desto geringer die Anzahl der notwendigen Überschreibungen) ab.

Vielen Nutzern ist nicht bewusst, dass ein einfaches Löschen („Delete“-Befehl, Verschieben in den Papierkorb, „Quick-Format“) der Daten daher in keinem Fall ausreichend ist. Zwar wissen die meisten Windows-Benutzer, dass ein Wiederherstellen eines Dokuments aus dem Papierkorb problemlos möglich ist. Den meisten ist aber nicht bewusst, dass auch nach Löschen des Papierkorbs und sogar nach Formatieren der Festplatte die Daten problemlos mit einer herkömmlichen Datenrettungs-Software wiederhergestellt werden können.

Es erfordert einen relativ hohen Aufwand, Informationen so nachhaltig zu vernichten oder unkenntlich zu machen, so dass sie definitiv – d.h. auch in entsprechend ausgestatteten Laboren – nicht mehr ausgelesen werden können.

Für die allermeisten Fälle gilt jedoch: Schon mit überschaubarem Aufwand kann eine sehr hohe Sicherheit erreicht werden. Mit Hilfe geeigneter Software können die Daten so überschrieben werden, dass eine Rekonstruktion der Daten wohl nur noch in absoluten Ausnahmefällen zu befürchten ist. Der zur Wiederherstellung der Daten notwendige Aufwand wäre so hoch, dass sich nur rechnen würde, wenn sehr hohe „Profite“ – wie z.B. bei Industriespionage – winken würden.

Für den Privatnutzer werden Software-Lösungen – z.T. auch als Freeware – angeboten, die eine hohe Sicherheit für die üblicherweise im privaten Umfeld vorhandenen Daten gewährleisten.

Eine Alternative zur Vermeidung des Datenmissbrauchs stellt die Verschlüsselung der Daten dar. Jedoch muss auch hier sichergestellt werden, dass alle sensitiven Daten verschlüsselt werden und der Schlüssel sicher verwahrt wird.

2.2 Datenlöschung mittels Software

Wie bereits oben angesprochen, bietet das „normale“ Löschen der Dateien keinen ausreichenden Schutz. Beim Verschieben von Dateien in den Papierkorb oder durch den „Delete“-Befehl werden die gespeicherten Daten nicht verändert. Es wird dabei lediglich der örtliche Verweis aus dem Inhaltsverzeichnis des Datenträgers entfernt, bzw. ein Kennzeichen zur Überschreiberlaubnis gesetzt. Die Daten sind also auf den ursprünglichen Plattensektoren weiterhin vorhanden und können wiederhergestellt und ausgelesen werden.

Auch beim Formatieren der Festplatte wird nur das Inhaltsverzeichnis (d.h. die Dateizuordnungstabelle) gelöscht, die Daten selbst bleiben unverändert. Das ist vergleichbar mit dem fehlenden Inhaltsverzeichnis in einem Buch: Es fehlt zwar die Möglichkeit, Informationen direkt anzusteuern, doch lesen kann man das Buch immer noch.

Bei einem „Low-Level-Format“ werden alle Datenbereiche mit einem einheitlichen Bitmuster überschrieben Mit geeigneten Geräten können aber die ursprünglichen Daten aus der Restmagnetisierung in den Randbereichen der Datenspuren wieder hergestellt werden.

Eine vollständige Löschung, die eine Wiederherstellung unmöglich macht, erzielt man nur durch mehrmaliges Überschreiben des Datenträgers mit unterschiedlichen Bitmustern. Für dieses Verfahren wurden auch mehrere Standards definiert:

- 5220.22-M-Standard des US-Verteidigungsministeriums (3faches Überschreiben)
  Bei diesem Verfahren wird die Festplatte im ersten Durchgang mit einem fest vorgegebenen und anschließend mit dem Komplementärwert überschrieben. Im letzten Durchgang wird die Festplatte mit Zufallszahlen überschrieben.

- VSITR-Standard des Bundesamt für Sicherheit/Informationstechnik (BSI) - 7faches Überschreiben
  Die Festplatte muss in 7 Durchgängen überschrieben werden. Zunächst wird die Festplatte mit einem zufälligen Bitmuster überschrieben. Anschließend wird in den nächsten 5 Durchgängen die Festplatten mit dem jeweils invertierten Bitmuster (d.h. jede 0 wird durch eine 1 und jede 1 durch eine 0 ersetzt) überschrieben. Im letzten Durchgang wird die gesamte Festplatte mit dem Muster „01010101“ überschrieben.

- Bruce-Schneier-Algorithmus - 7faches Überschreiben
  Bei diesem Verfahren wird die Festplatte zunächst mit binären Nullen, anschließend mit binären Einsen überschrieben. In den 5 verbleibenden Durchgängen wird die Festplatte mit zufällig erzeugten Bitmustern überschrieben.

- Der Vorteil dieses Verfahrens gegenüber dem ähnlichen VSITR-Standard besteht darin, dass die zufälligen Bitmuster das Aufspüren eventueller Restmagnetisierungen an den Rändern wesentlich erschweren.

- Peter-Gutmann-Algorithmus
  Bei diesem Algorithmus wird die Festplatte 35mal überschrieben. Dieses hohe Maß an Sicherheit nimmt allerdings auch wesentlich mehr Zeit in Anspruch. Anzumerken ist, dass die Untersuchungen von Peter Gutmann vor mehr als 10 Jahren durchgeführt wurden. Zu dieser Zeit war die Speicherdichte auf den Festplatten wesentlich geringer und damit die Breite der magnetisierten Spuren wesentlich breiter als heute.

Professionelle Lösungen der auf dem Markt erhältlichen Software zur Datenlöschung bieten ausführliche Reportingfunktionen, die Verifizierung der erfolgreichen Löschung und Nachweise über die erfolgten Löschvorgänge. Zudem können Parameter und Löschalgorithmen ausgewählt oder selbst definiert werden. Löschungen über das Firmennetzwerk zu betreiben, ist ein Plus einiger Softwarelösungen. Ebenso wie die Möglichkeit, externe Festplatten und Flash-Speicher via USB und Firewire zu löschen.

Bei allen Löschvorgängen mit Software bleibt jedoch ein geringes Restrisiko. Jede Festplatte generiert im Laufe ihres Lebens sogenannte „bad blocks“ also schlechte Datenblöcke. Die Menge ist abhängig von Modell und Festplattenalter. Die darin enthaltene Information wird von der Firmware automatisch kopiert. Da diese Blöcke nicht mehr angesprochen werden, bleiben sie auch bei einer Löschung mit Software unangetastet. Besonders im Bereich der Computer Forensik, der Beweisermittlung digitaler Daten und deren gerichtsverwertbarer Analyse, können sich hier wertvolle Hinweise verbergen.

2.3 Datenlöschung durch Hardware

2.3.1 Schredder

Eine zuverlässige Methode zur endgültigen Datenlöschung ist die physikalische Zerstörung von Datenträgern. Eine gängige Methode ist das sogenannte Schreddern. Ein Schredder (englisch: shredder) ist ein mechanisches Gerät zum Zerkleinern von unterschiedlichsten Materialien. Das bedeutet, der Datenträger wird zerstört, indem er in kleine Teile zerlegt wird.

2.3.2 Degausser

Eine weitere Möglichkeit zur nachhaltigen Löschung ist die Entmagnetisierung mittels eines Degaussers. Ein Degausser ist ein elektrisches Gerät, mit dessen Hilfe magnetische Datenträger durch Entmagnetisierung zuverlässig gelöscht werden können. In einem Degausser wird der Datenträger einem starken Magnetfeld ausgesetzt. Der Name Degausser geht auf die Einheit der magnetischen Flussdichte, das Gauss, zurück.

Festplatten, Disketten und Bänder werden in wenigen Sekunden entmagnetisiert: Alle darauf befindlichen Informationen werden unwiederbringlich gelöscht. Dies gilt auch für die Servo- und Wartungsinformationen der Festplatten, was bedeutet, dass die Platten danach nicht mehr eingesetzt werden können. Die Medien können umweltgerecht entsorgt werden.

2.3.3 Thermische Zerstörung

Wird die Oberfläche der Magnetplatte über die Curie-Temperatur der verwendeten Beschichtung (z.B. bei Eisen 766 °C) erhitzt, verliert das Material seine magnetische Eigenschaft und die Daten werden unwiderruflich gelöscht.

2.4 Vorteile / Nachteile bei Datenlöschung durch Hardware

Ein klarer Vorteil der Löschung durch Schredder, Degausser oder thermische Zerstörung ist, dass auch beschädigte Festplatten, die vom Betriebssystem nicht mehr erkannt und damit von einer Software auch nicht mehr ansprechbar sind, sicher gelöscht werden können. Ansonsten besteht die Möglichkeit, Daten von physikalisch beschädigten Platten in spezialisierten Datenrettungslabors wieder herzustellen.

Die Hardware-basierten Datenlöschverfahren führen aber immer zur Zerstörung der Magnetplatte, ihre Weiterverwendung – auch eine ggf. geplante Fehleranalyse bei defekten Geräten – ist daher ausgeschlossen.

2.5 „Do-it-yourself“ oder Dienstleistungsunternehmen?

Prinzipiell kann das Löschen oder Vernichten der Datenträger entweder selbst oder von einem Dienstleistungsunternehmen vorgenommen werden. Bei Privatpersonen wird sich häufig die „Do-it-yourself“-Lösung mittels Software anbieten, während Unternehmen allein schon wegen der dafür benötigten Zeit und der Menge anfallender Datenträger auf netzwerkfähige Softwarelösungen, Schreddern oder Degausser zurückgreifen. Auch der Service durch Datenlöschunternehmen ist eine Möglichkeit, wenn die Daten das Unternehmen verlassen dürfen. Im professionellen Umfeld ist es auch immer wichtig, dass die Löschvorgänge durch Zertifikate und Reports – z.B. unter Angabe der Seriennummern der Festplatten – jederzeit nachvollzogen und belegt werden können.

3 Resümee / Empfehlung für eine sichere Datenlöschung

Um zu vermeiden, dass Informationen auf Datenträgern, die im Unternehmen oder bei Privatpersonen nicht mehr verwendet werden, nicht von Unberechtigten gelesen werden, sollten diese grundsätzlich vor der Ausmusterung gelöscht werden. Die vom Betriebssystem angebotenen Befehle (delete, format, fdisk, etc.) sind dafür nicht ausreichend, da sie nur die Inhaltsverzeichnisse der gespeicherten Dateien löschen, die eigentlichen Daten aber nach wie vor auf dem Datenträger gespeichert bleiben (und mit entsprechenden Softwaretools leicht wieder restauriert werden können).

Handelt es sich bei den gespeicherten Informationen um streng geheime oder äußerst sensible Daten?

- Ja: Die Datenträger (inkl. der „bad blocks“) sollten nicht mehr rekonstruiert werden können. Die dafür zur Verfügung stehenden Methoden zerstören aber den Datenträger soweit, dass eine spätere Weiterverwen-dung ausgeschlossen ist. Die zur Verfügung stehenden Methoden sind:
  - Löschen der Daten durch Einsatz eines sehr starken Magnetfelds („Degausser“),
  - Abfräsen der Beschichtung auf den Magnetplatten,
  - Erhitzen der Magnetplatten über die Curietemperatur,
  - Schreddern der Magnetplatte (Achtung: Sind die entstehenden Fragmente nicht klein genug, so lässt sich daraus ein Großteil der Informationen wiedergewinnen.).

- Nein: Die gesamte Festplatte sollte mit Hilfe einer speziellen Software mit unterschiedlichen Bitmustern überschrieben werden.

Es gibt auf dem Markt auch Dienstleistungsunternehmen, die eine Kombination der aufgeführten Maßnahmen (z.B. Schreddern und Einschmelzen etc.) anbieten.

Für die Löschung von Datenträgern mittels Software existieren etliche Tools, die als Download im Internet oder im Fachhandel erhältlich sind. Qualitativ weisen sie aber untereinander große Unterschiede auf. Mit ihnen werden die Datenbereiche mehrfach mit unterschiedlichen Bit-Mustern überschrieben. Beim Kauf sollte darauf geachtet werden, dass die Software dem jeweiligen Bedarf, z.B. Löschen von Speicherkarten, Löschen über Netzwerk, Generieren von Reports, gerecht wird. Der für OS und BIOS reservierte Bereich sollte auch überschrieben werden.

Auch bei optischen Datenträgern (CDs, DVDs) und Flash-Medien empfiehlt sich häufig die Zerstörung der Datenträger, bevor diese in andere Hände gelangen können. Während bei den optischen Medien die Datenträgerschicht für eine Löschung beschädigt werden muss, ist auch bei der Vernichtung von Flash-Medien wie USB-Sticks der physikalische Aufwand nicht zu unterschätzen.

Zusammenfassend lassen sich folgende Empfehlungen abgeben:

- Sollen Festplatten weiter verwendet werden, etwa in einer anderen Abteilung, Rückgabe des Laptop an die Leasingfirma oder Weiterverkauf, so sind sie mit einem geeigneten Softwaretool komplett zu überschreiben, mindestens dreimal - bei hochsensiblen Daten siebenmal.
- Bei hochsensiblen Daten ist immer eine physikalische Zerstörung der Datenträger in Erwägung zu ziehen.
- Defekte Datenträger sollten vor deren Entsorgung grundsätzlich immer zerstört werden, bevor Daten in die Hände von unbefugten Dritten gelangen könnten.
- Bei Abgabe der Rechner/Festplatte zu Reparaturzwecken sollte man sich mit einem „Datenschutz-Revers“ absichern. Darin verpflichtet sich der Dienstleister, alle Datenschutzvorschriften einzuhalten, insbesondere die auf dem Datenträger gespeicherten Daten zu keinem anderen Zweck zu verwenden, sie weder

zu kopieren noch an Dritte weiterzugeben. Im Revers sollte eine entsprechend hohe Konventionalstrafe vereinbart sein.

- Werden Daten an Dritte weitergegeben, sollten möglichst neue Datenträger (z.B. Disketten) verwendet werden. Ist dies nicht möglich, so sollte der Datenträger mehrfach überschrieben werden und keinesfalls nur formatiert werden.
- Eine lückenlose Dokumentation der Datenlöschung sollte – zumindest beim Einsatz im gewerblichen Umfeld – unbedingt erfolgen. Denn wer Compliance-Kriterien erfüllen will, muss seine Handlungen immer dokumentieren können – bestenfalls sogar mit einem manipulationssicheren Report.

4 Weitere Informationen / Links

Weitere Informationen zum Thema sind z.B. bei folgenden Quellen zu finden:

BITKOM-Leitfaden zur IT-Sicherheit
http://www.bitkom.org/de/publikationen/38337_38229.aspx

Bundesamt für Sicherheit in der Informationstechnik
www.bsi.de

Sicheres Löschen von Datenträgern – IT Grundschutzkataloge
http://www.bsi.de/gshb/deutsch/m/m02167.htm

Kroll Ontrack Whitepaper Datenlöschung und Handbuch Degausser
www.ontack.de/eraser

SearchStorage Datenlöschung ist das zweite Standbein der Datensicherheit
http://www.searchstorage.de/themenkanaele/primarystoragehardware/allgemein/articles/66316/

SearchStorage Datenshredder für Interna
http://www.searchstorage.de/themenkanaele/storagesecurity/allgemein/articles/49754/

Garfinkel-Studie „Remembrance of Data Passed“
http://www.computer.org/security/garfinkel.pdf

Gutmann: Secure Deletion of Data from Magnetic and Solid-State Memory
http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html

Tecchannel
http://www.tecchannel.de/software/1161/index.html

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.200 Unternehmen, davon 900 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software, IT-Services und Telekommunikationsdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für bessere ordnungspolitische Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.

BITKOM

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org