Datenvernichtung - Sie möchten Ihre Daten dauerhaft vernichten oder entsorgen? Wir haben die Lösung.

Der Diebstahl von "angeblich" gelöschten Daten nimmt immer mehr zu. Dadurch kommt es vermehrt zu einer großen Bedrohung für die betroffenen Unternehmen. Schützen Sie Ihr Unternehmen gegen diesen Datenklau. Der mobile Datenshredder vermindert das Risiko von Informationsdiebstahl zu 100%, und das in nur wenigen Minuten. Ähnlich wie bei der Aktenvernichtung
wird hier eine mechanische Zerkleinerung zur Datenvernichtung eingesetzt.

Warum ist die mechanische Löschung die sicherste Datenvernichtung?

Gelöschte Informationen auf Datenträgern wie Storage-Systeme, HD, DVD, CD und Magnetbändern sind nicht wirklich physikalisch gelöscht! In aller Regel wird hier nur das Inhaltsverzeichnis des Datenträgers zerstört. Die Files können sehr leicht mit Wiederherstellungs-Tools sichtbar gemacht werden.
Wir vernichten die Datenträger mechanisch, hier bleibt weder die Elektronik noch das Medium selbst ganz! Eine Wiederherstellung dieser Zerstörten Daten ist unmöglich. Diese sind dann unwiederbringlich und endgültig zerstört.

- Die *recycle it GmbH* bietet Ihnen hierfür die Lösung durch unseren **mobilen Datenshredder** als Serviceleistung direkt an Ihrem Standort.

- Wir führen die **Vernichtung** Ihrer digitalen Datenträger mittels eines **2-stufigen Shredderkonzepts**
durch.

- Der erste Harddisk Shredder zerkleinert die Medien diese Daten mit sog. normalem Schutzbedarf beinhalten, in kleine Streifen.
Die Partikelgrößen hierfür liegen bei 300 - 900 Quadrat Millimeter. Wir nennen diese Art der **Datenträgervernichtung**

- Standard-Service.

- Ein weiterer Datenshredder auf dem DATENKILLER ist mit Zweiwelle und Siebeinsatz ausgestattet. Dieser gewährleistet dann anschließend in einem zweiten Prozess die Zerkleinerung der Festplatten mit einer Partikelgröße von <=10 Quadrat Millimeter. Dies ist notwendig für Festplatten mit sog. hohem Schutzbedarf. Diese Art der **Datenträgervernichtung** nennen wir **Premium- bzw. Premium++-Service** und bedeutet die sicherste Art der Daten Vernichtung!

- **Zu Ihrer Sicherheit**: wir sind mehrfach zertifiziert und die Datenvernichtungsprozesse werden jährlich durch die LGA InterCert zusätzlich überprüft und auditiert.

- Je nach gewünschter Vernichtungsart bekommen Sie **kostenlos** ein detailliertes **Datenvernichtungs-Zertifikat** nach dem Standard- oder dem Premium- bzw. Premium++-Service mit Nachweis sämtlicher **Seriennummern** aller vernichteten Festplatten, sowie **zusätzlich ein Recyclingzertifikat** für die anschliessende abfallrechtliche Verwertung des Restmaterials.

- Zusätzlich können wir die Möglichkeit einer **Videoüberwachung** des gesamten Vernichtungsvorgangs anbieten. Dabei ist unser mobiles Fahrzeug mit einer Videokamera ausgestattet, die es Ihnen ermöglicht das Entsorgen in Echzeit zu verfolgen und den **Film dann auf eine SD-Karte** laden zu lassen. Nach dem Vernichtungsprozess kann Ihnen der Film mit der SD-Karte überreicht werden. Die Dienstleistungspauschale für diese Option erhalten Sie auf Anfrage.

Wie ist die Datenträgervernichtung nach DIN EN 66399 definiert?

Festplattenvernichtung - Datenträgervernichtung

Haben Sie sich schon mal Gedanken darüber gemacht, wenn Sie Ihren alten Computer zum Wertstoffhof bringen, was dann mit Ihren Daten auf der Festplatte alles passieren kann? Findet hier wirklich eine sichere **Datenträgervernichtung** statt?

Und was wissen Sie noch über Ihren alten Computer?

- Welche persönlichen Dateien könnten sich noch auf dem elektronischen Gerät befinden?

- Sind Ihre Bankdaten noch auf dem Datenträger gespeichert?

- Sind wichtige Arbeitsunterlagen noch auf Ihrem privaten PC hinterlegt?

- Oder aber, welche persönlichen Fotos befinden sich noch auf der Harddisk, die auch wirklich persönlich bleiben sollten?

- Könnten Sie die Datenträgervernichtung selbst durchführen?

- Wie findet eine sichere Datenlöschung statt?

Zu viele Fragen?

Wir denken nicht.
Nachweislich denken die wenigsten Verbraucher an den Schutz Ihrer eigenen persönlich gespeichterten Informationen, wenn sie Ihren Computer am Wertstoffhof abgeben, da die meisten Bürger davon ausgehen, daß nach einem ordnungsgemäßen Recycling auch die Daten entsorgt sind.

Dies ist aber in der Realität meist nicht der Fall.

Ein abfallrechtliches Recycling gem. dem neuen ElektroG beinhaltet nicht automatisch die fachgerechte Datenlöschung und kann unter Umständen auch das umweltgerechte Wiederverwenden einzelner Computerteile, unter anderem auch einer Harddisk, beinhalten. Was würden Sie davon halten, wenn Ihre persönlichen Dateien im Rahmen eines Wiederverkaufs beispielsweise bei ebay wieder auftauchen würden?

Welche Möglichkeiten gibt es nun sich vor einem solchen Datenmissbrauch zu schützen?

1. Datenlöschung mittels Software

Der „normale“ Papierkorb oder das Formatieren der Harddisk mittels des Betriebssystems bietet keinen ausreichenden Schutz, kostenlose Tools können diese Dateien ganz einfach wiederherstellen. Beim Verschieben von Dateien in den Papierkorb oder durch den einfachen „Delete“-Befehl werden die gespeicherten Files nicht gelöscht. 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 Datei-Zuordnungstabelle) geleert, die Informationen selbst bleiben unverändert.

Was für eine Datenlöschung ist demnach sinnvoll?
Ein vollständiger Datenschutz, der eine Wiederherstellung unmöglich macht, und die Informationen vernichtet, erzielt man nur durch mehrmaliges Überschreiben des Datenträgers mit unterschiedlichen Bitmustern.
Dazu gibt es spezielle Softwarelösungen.
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.
Wir empfehlen dabei immer mindestens ein dreimaliges Überschreiben der Festplatten. Nur so ist die Datenlöschung mittels einer Software wie z.B. eraser akzeptabel.

Und gibt es dann immer noch ein Risiko?
Bei allen Löschvorgängen mit Software bleibt nach wie vor 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 Datenlöschung mit Software unangetastet. Besonders im Bereich der Computer Forensik, der Beweisermittlung digitaler Daten und deren gerichtsverwertbarer Analyse, können sich hier wertvolle Hinweise verbergen.

Wie findet eine sichere Datenlöschung statt?

Was gibt für weitere der Möglichkeiten der Datenträgervernichtung bzw. Festplattenvernichtung?

2. Datenlöschung durch Hardware

2.1 Degausser

Was ist ein Degausser?
Eine weitere Möglichkeit zur nachhaltigen Löschung von digitalen Datenträgern ist die Entmagnetisierung mittels eines Degaussers. Ein elektrisches Gerät, mit dessen Hilfe magnetische Datenträger durch Entmagnetisierung zuverlässig neutralisiert werden können. In diesem Gerät 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 nach wenigen Sekunden entmagnetisiert: Alle darauf befindlichen Informationen werden dadurch gelöscht. Dies gilt auch für die Servo- und Wartungsinformationen der Festplatten, was bedeutet, dass die Festplatten danach nicht mehr eingesetzt werden können.

Worin liegt das Risiko eines Degaussers?

Da wäre zum einen der Anwender: die Festplatte muss je nach Magnetfeldstärke für eine gewisse Verweildauer dem Magnetfeld des Degausser ausgesetzt sein. Ist die Verweildauer zu gering kann es sein, dass nicht alle Daten gelöscht worden sind. Da die Festplatte optisch nicht zerstört ist, sieht man ihr nicht an, ob die Daten vernichtet wurden oder nicht. Daten der neuen Bauart von SIS-Festplatten können aufgrund der technischen Gegebenheiten nicht über einen Degausser gelöscht werden.

2.2 Datenvernichtung durch 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 vernichtet. Auch hier sprechen wir von einer Datenträgervernichtung.

2.3 Datenvernichtung durch mechanische Shredder

Eine sehr zuverlässige Methode zur endgültigen Datenlöschung ist die physikalische Zerstörung von Datenträgern. Eine gängige Methode ist das sogenannte Schreddern. Ähnlich

wie bei der Aktenvernichtung werden hier die digitalen Akten durch einen Datenshredder in kleine Stücke zerteilt.
Der 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.

Worin sind die Vorteile bzw. Nachteile?

Ein klarer Vorteil der Datenvernichtung durch den Schredder, Degausser oder thermischen Zerstörung ist, dass auch beschädigte Festplatten, die vom Betriebssystem Windows, Unix, usw. nicht mehr ansprechbar sind, sicher unbrauchbar gemacht werden können.
Ansonsten besteht die Möglichkeit, Dateien von physikalisch beschädigten Platten in spezialisierten Datenrettungslabors wieder herzustellen.

Die hardwarebasierten Datenlöschverfahren führen immer zur Zerstörung der Magnetplatte, ihre Weiterverwendung – auch eine ggf. geplante Fehleranalyse defekter Geräte – ist daher ausgeschlossen. Hier sprechen wir von der endgültigen Datenentsorgung.

3. Wie sieht nun die praxisgerechte Empfehlung aus?

Datenlöschung oder Datenträgervernichtung im do-it-yourself-Verfahren?

oder aber

Beauftragung eines professionellen Dienstleistungsunternehmens?

Wo bekomme ich eine sichere Datenentsorgung?

Prinzipiell kann das Vernichten der elektronischen Medien 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 Datenträgern auf netzwerkfähige Softwarelösungen, Schreddern oder Degausser zurückgreifen.

Auch die Dienstleistung eines externen Datenlöschunternehmen ist eine Möglichkeit, wenn die Daten das Unternehmen verlassen dürfen. Hier findet die Vernichtung im sicheren Entsorgungs- und Vernichtungszentrum statt.

Im professionellen Umfeld ist es auch immer wichtig, dass die Löschvorgänge und Datenträgervernichtungen durch Zertifikate und Reports – z.B. unter Angabe der Seriennummern der Festplatten – jederzeit nachvollzogen und belegt werden können.

Autor: recycle it GmbH
Fachgebiet: Datenträgervernichtung und Entsorgung elektronischer Medien
www.recycle-it.de
www.datenkiller.com

Quelle: BitKom – Leitfaden zum sicheren Datenlöschen