SearchSecurity.de

Maximale Sicherheit bei der Datenvernichtung

Die Festplatte muss in den Reisswolf

22.12.2008 | Redakteur: Peter Schmitz

Nur die physische Zerstörung eines Datenträgers garantiert absolute Datensicherheit.

Was für Papierdokumente bereits Standard ist, setzt sich langsam auch für Festplatten durch: Das Shreddern. Dass das einfache Löschen von Dateien oder Formatieren von Festplatten keinen wirklichen Sicherheitsgewinn darstellt weiß man längst. Löschsoftware mit der komplette Datenträger überschrieben werden ist die kostengünstigste Methode Datensicherheit auf ausgemusterten Festplatten zu erreichen, aber sicherer ist die physische Zerstörung im Reisswolf.

Inzwischen bewegt das Thema Datensicherheit und Forensik sogar das alltägliche Geschäftsleben, wie folgender Fall beweist: Ein Konzern wollte auf Nummer sicher gehen und alle Beweise darüber, wie er das komplette Management eines Konkurrenzunternehmens abgeworben hatte, vernichten. Alle Festplatten, auf denen verräterische Daten über den Vorgang gespeichert waren, wurden gelöscht, formatiert und überschrieben. Dennoch konnte von einem Datenrettungsspezialisten ein Dokument, das den unlauteren Wettbewerbs belegte, wiederhergestellt werden. Die geschädigte Firma zog vor Gericht.

Was aber in diesem Fall als Glücksfall für die Justiz bezeichnet werden kann, bereitet dem unbescholtenen Bürger eher Unbehagen. „Das Thema Datenschutz ist zurzeit ein Hype. Gleichzeitig ist die Sensibilität für den Umgang mit den eigenen Daten noch nicht vorhanden, “ sagt Maximilian Scheppach, Geschäftsführer der auf Datenvernichtung spezialisierten recycle it GmbH. „Firmen sehen sich vor allem durch Sorglosigkeit im Umgang mit Festplatten bedroht. So lange die Speichermedien nicht vollständig und zuverlässig zerstört werden, besteht die Gefahr, dass Daten wie Geschäftsberichte, Konstruktionszeichnungen, Transaktionen oder Passwörter in die falschen Hände geraten.“

„Erstaunlich, wie wenig Sorgfalt viele Menschen walten lassen, wenn es um den Schutz ihrer persönlichen oder geschäftlichen Daten geht. Und das, wo doch viele Bürger Angst davor haben, „gläsern“ zu werden. Sie fürchten, dass der Staat in unkontrollierbarem Ausmaß Einsicht in ihre privaten Daten erlangt. Die Sorge um den Datenschutz ist berechtigt.“, so Scheppach weiter.

In Großbritannien gab es in diesem Jahr eine Reihe von Skandalen in diesem Zusammenhang. So ersteigerte der IT-Berater Andrew Chapman etwa ganz legal auf eBay Festplatten, auf denen er dann sensible Informationen von mehr als einer Million Bankkunden fand. In einem anderen Fall ersteigerte eine Person eine Festplatte, auf der zehntausende Dateien mit persönlichen Daten zahlreicher Bürger der englischen Gemeinde Charnwood abgespeichert waren. Die Daten auf dieser Festplatte waren gelöscht, konnten aber mit handelsüblicher Software wiederhergestellt werden.

Bildergalerie



Klicken Sie auf ein Bild um die Bildergalerie zu öffnen (3 Bilder)

Einfache Informationsgewinnung aus der Mülltonne

In Deutschland sieht es kaum anders aus Eine Studie des Softwareherstellers O&O-Software zum Datenschutz bei gebrauchten Festplatten vom September 2007 kam zu dem Ergebnis, dass von fast 400 ersteigerten Datenträgern aus Internetauktionen mehr als 66% aller Festplatten persönliche und geschäftliche Daten ihrer Vorbesitzer enthielten.

Informationen liefern, die sich auf Festplatten persönliche und geschäftliche Daten ihrer Vorbesitzer befinden.

Auch in einem Dokument des IT- Grundschutzkatalogs des Bundesamtes für Sicherheit in der Informationstechnik (BSI) heißt es: „Angreifer müssen nicht immer komplizierte technische Attacken austüfteln, um über Schwachstellen in IT-Systemen an Informationen zu gelangen. Viel einfacher und erfolgreicher kann die Informationsgewinnung aus der Mülltonne sein."

Seite 2: Die Grenzen von Löschsoftware

Die Grenzen von Löschsoftware

„Eine rückstandsfrei gelöschte Festplatte gibt es in der Regel nicht, " sagt auch Diplom-Ingenieur Nicolas Ehrschwendner, Geschäftsführer der auf Datenrettung spezialisierten Wiener Firma „Attingo", der die Wiederherstellung des kompromittierenden Word-Dokuments über die abgeworbenen Mitarbeiter der Konkurrenz gelang. Zwar gäbe es die Möglichkeit des Überschreibens der Festplatte, jedoch warnt Ehrschwendner: „Wann immer in einem physikalischen Bereich der Festplatte ein Defekt auftritt, wird er elektronisch abgetrennt, und die Daten werden in einen Ersatzbereich kopiert. Auf diese gesperrten Bereiche kann vom System nicht mehr zugegriffen werden. Es gibt derzeit keine Löschsoftware, die sie überschreiben kann."

Auch der Slack space, der ungenutzte Speicherplatz innerhalb eines Datenclusters, wird nicht von allen Löschprogrammen überschrieben. DOS und Windows Systeme arbeiten mit festgelegten Datenblocklängen. Wenn die tatsächliche Dateigröße kleiner ist als in so einem Cluster zur Verfügung steht, wird trotzdem das gesamte Cluster für die Datei reserviert und der zur Verfügung stehende Platz willkürlich und ohne direkten Einfluss des Anwenders mit Daten aus verschiedenen Bereichen des Systems aufgefüllt.

Der Slack Space wird dann nicht überschrieben, wenn der Anwender mit einer Löschsoftware nur gezielt bestimmte Dateien löscht. Wenn die Software den gesamten Datenträger löschen soll, wird in der Regel auch der Slack Space überschrieben, da die Software dann jeden Sektor (in der Regel 512 Bytes) überschreibt. Wenn man eine Datei mit Löschsoftware löscht (z.B. 400 Bytes), dann werden oft nur die 400 Bytes gelöscht, jedoch nicht Daten, mit denen der Sektor vorher einmal beschrieben war. In computerforensischen Untersuchungen spielt der Slack space eine große Rolle, da man mit ihm womöglich sensible Daten extrahieren kann.

Das letzte Experiment der Columbia

Eine weitere Möglichkeit wäre das Einschmelzen oder Verbrennen der Festplatte. Doch auch hier gelingt zuweilen die Datenrettung: Im Februar 2003 verglühte die US-Raumfähre Columbia beim Wiedereintritt in die Erdatmosphäre. Sie bewegte sich zum Zeitpunkt des Auseinanderbrechens mit 20.000 Stundenkilometern, ihre Wrackteile verteilten sich über hunderte von Kilometern. Zwei Metallteile, davon eine Festplatte, waren miteinander verschmolzen und durch einen 60-Kilometer-Sturz verbeult. Trotzdem gelang es Datenrettungsexperten, Informationen von dieser Festplatte zu rekonstruieren. Fünf Jahre nach dem Absturz konnten schließlich die kompletten Ergebnisse des letzten dokumentierten Experiments der Columbia-Crew veröffentlicht werden.

Bildergalerie

Klicken Sie auf ein Bild um die Bildergalerie zu öffnen (3 Bilder)

Seite 3: Sicherheit durch Shreddern

Sicherheit durch Shreddern

Eine andere Methode der Datenvernichtung ist das Entmagnetisieren der Festplatte durch einen so genannten Degausser. Jedoch wird die Festplatte dabei physisch nicht zerstört, eine Garantie dafür, dass der Degausser wirklich alle Daten vernichtet hat, gibt es daher nicht.

Will man sich der Vernichtung seiner Daten sicher sein, gibt es derzeit nur eine zuverlässige Methode, wie Scheppach erklärt: „Das Non plus ultra bei dem Thema ist die physische Zerstörung der Festplatten." Der unter dem Namen „Datenkiller" firmierende Geschäftszweig seiner recycle it GmbH bietet die mobile mechanische, fachgerechte

„Datenkiller" – firmierende Geschäftszweig seiner recycle it GmbH bietet die mobile mechanische, fachgerechte Datenvernichtung von Festplatten und anderen digitalen Datenträgern an: Sicherheit durch Shreddern.

Festplatten, die zerstört werden sollen, müssen nicht transportiert werden. Der „Datenkiller" kommt in das Unternehmen. Die verantwortlichen Mitarbeiter können den Vernichtungsvorgang überwachen, laut Scheppach gilt stets das „vier Augen Prinzip".

Bildergalerie

Klicken Sie auf ein Bild um die Bildergalerie zu öffnen (3 Bilder)

Verwendet wird ein so genannter „Hard Disk Terminator" der Firma Erdwich Zerkleinerungssysteme GmbH aus Kaufering. Es handelt sich hierbei um eine spezielle Zerkleinerungsmaschine mit massivem Präzisionsschneidwerk. Die Festplatten werden einzeln über eine spezielle Zuführöffnung in die Maschine gegeben. Zwei entgegenlaufende Messerwellen erfassen und zerkleinern das Material. Die nach der Zerkleinerung übrig bleibenden Fragmente weisen dann nur mehr eine Fläche von etwa 600 mm² bis 900mm² auf und sind stark verformt. Eine Rekonstruktion ist in der Praxis unmöglich. Dies bestätigte auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) in einem Gutachten.

Recycling statt Müll

Ein weiterer Vorteil der Methode ist, dass durch die Zerkleinerung die Wertstoffe getrennt und so der Wiederaufbereitung zugeführt werden können. Der Geschäftsführer der Erdwich Zerkleinerungssysteme GmbH Hans Erdwich erklärt, dass die Recyclingquote bei bis zu 95% liegt. Von Metallaufbereitern wird das Material getrennt und z.B. zur Kupferverhüttung und dem Aluminiumschmelzwerk gegeben. Damit stellt das Shreddern nicht nur eine sichere, sondern auch umweltfreundliche Methode der Datenvernichtung dar. Insbesondere im Hinblick auf die neue WEEE Richtlinie (Waste Electrical and Electronic Equipment) der EU ein großer Pluspunkt.