Sicherheit

Löschsoftware ist unsicher – Sogar verbrannte Disks lassen sich rekonstruieren – Nur Shreddern zerstört Daten zuverlässig

Sorgloser Umgang mit alten Festplatten bedroht Firmen

04. November 2008

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. Was für Papierdokumente bereits Standard ist, setzt sich langsam auch für Festplatten durch: Shreddern.

_Der Terminator – für Festplatten: Der Einwurf oben rechts ist die letzte Station im Leben einer Disk. Danach bleibt nur recyclingfähes Material übrig, aus dem sich keinerlei Daten mehr rekonstruieren lassen. Foto: Erdwich Zerkleinerungssysteme

Der Konzern wollte auf Nummer sicher gehen und alle Beweise darüber, wie er das komplette Management eines Konkurrenzunternehmens abgeworben hatte,

vernichten. Die Festplatte mit den verräterischen Daten wurde überschrieben, fragmentiert und gelöscht. Dennoch konnte ein Dokument, das den unlauteren Wettbewerbs belegte, von Datenrettungsspezialisten 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 Recycle it GmbH, die sich in einem Geschäftsbereich auf die Datenvernichtung spezialisiert hat. Firmen sehen sich vor allem durch Sorglosigkeit im Umgang mit Festplatten bedroht.

Mehr zum Thema

Backup-Bänder sind trotz Datenverluste weiter ungeschützt

SAP und Cisco präsentieren gemeinsame Anwendung für Datenschutz und Datensicherheit

HP erweitert seine Lösung für Festplattenverschlüsselung und Schlüsselverwaltung

Anbieter wollen Verschlüsselung im Speicherbereich vorantreiben

Dabei ist es schon erstaunlich, wie viele Menschen mit dem Schutz ihrer persönlichen oder geschäftlichen Daten umgehen. 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.

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. Diese Festplatte war gelöscht gewesen, jedoch mit handelsüblicher Software wiederhergestellt worden.

In Deutschland sieht es kaum anders aus: Computerbesitzer scheinen sich sogar mehrheitlich keine Gedanken darüber zu machen, in wessen Hände ihre vertraulichen Daten gelangen können. Denn die O&O- Studie zum Datenschutz bei gebrauchten Festplatten vom September 2007 kam zu dem Ergebnis, dass von fast 400 ersteigerten Datenträgern aus Internetauktionen mehr als 66 Prozent aller Festplatten persönliche und geschäftliche Daten ihrer Vorbesitzer enthielten.

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."

„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 werde der Slack Space, zu Deutsch Schlupfspeicher, nicht immer überschrieben. DOS und Windows Systeme arbeiten mit festgelegten Datenblocklängen (genannt Cluster). Wenn die tatsächliche Dateigröße kleiner ist als im Cluster zur Verfügung stände, 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 (zum Beispiel 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 Schlupfspeicher eine große Rolle, da man mit ihm womöglich sensible Daten extrahieren kann.

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

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. Und doch gelang es Experten, Daten dieser Festplatte zu rekonstruieren. Fünf Jahre nach dem Absturz konnten die Ergebnisse des letzten dokumentierten Experiments der Columbia-Crew veröffentlicht werden.

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 optische beziehungsweise physische Zerstörung der Festplatten.“ Der unter dem Namen 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 dabei nicht unbedingt transportiert werden: Der Datenkiller kommt in das Unternehmen. Die verantwortlichen Mitarbeiter können den Vernichtungsvorgang überwachen, laut Scheppach gilt stets das „vier Augen Prinzip“.

Verwendet wird dabei beispielsweise ein so genannter Hard Disk Terminator, wie ihn die Erdwich Zerkleinerungssysteme GmbH aus Kaufering einsetzt. 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. Zudem können bei dieser Methode die Wertstoffe getrennt und der Wiederaufbereitung zugeführt werden – mit einer Recyclingquote von bis zu 95 Prozent 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) ein großer Pluspunkt.