

le Roboter:
d zu mehr Qualität

Kettentransportsystem: Stückgut
flexibel in alle Richtungen transportieren

Schweißnaht vorbereiten
anbringen ohne Stau

NEWS

IT-Sicherheit

Sicherheitsrisiko Festplatte

Produktion Nr. 20, 2009

MÜNCHEN (sm). Firmen sind durch Sorglosigkeit im Umgang mit Festplatten bedroht. So lange die Speichermedien nicht vollständig zerstört werden, besteht die Gefahr, dass sensible Daten in die falschen Hände geraten. Was für Papierdokumente bereits Standard ist, setzt sich langsam auch für Festplatten durch: Shreddern.

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% 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 austüfeln, 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 Nicolas Ehrschwendner, Geschäftsführer der auf Datenrettung spezialisierten Wiener Firma ‚Attin-go‘, 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 Löschoftware, die sie überschreiben kann.“ Auch werde der Slack Space, zu Deutsch ‚Schlupfspeicher‘, nicht immer überschrieben. DOS und Windows-Systeme arbeiten mit festgelegten Datenblocklängen (genannt Clus-



Alte Festplatten sind eine beliebte Informationsquelle für Datenspione. Sie sollten deshalb durch Schreddern physikalisch zerstört werden.

ter). Wenn die tatsächliche Dateigröße kleiner ist als der Speicherplatz, der im Cluster zur Verfügung steht, wird trotzdem der 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 Löschoftware nur gezielt bestimmte Dateien löscht.

Das Nonplusultra ist die Zerstörung der Festplatte

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 Löschoftware 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 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. Will man sich der Vernichtung seiner Daten sicher sein, gibt es derzeit nur eine zuverlässige Methode, wie Scheppach erklärt: „Das Nonplusultra bei dem Thema ist die optische bzw. 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.

@ Sagen Sie uns Ihre Meinung: redaktion@produktion.de

TECHNIKBILD DER WOCHE



EU-Telekom-Paket

Gefährdung des Internets durch EU

von Sabine Spinnarke
Produktion Nr 20, 2009

des BVDW in sämtlichen Bereichen des Internets zu massiven Beschrän-

5-A
Ho

Prod

WEIN

freul
und 3
5-Ach
zagt i
ders
zugs
schän
„nutz
lich r
ne C
werb
volle
Zu
arbei
ser u
zagt
mons
ken
Naka



Leist
vielfä
Besu

weitr
bis h
arbei
lung
vortr
groß
Ther
zieru
nige
te d
Mas
schw
Haus
arbei
nen
indiv
nanz