Wenn der Müllmann zweimal klingelt...

Ausgeklügelte Backup-Strategien, redundante Systeme, hochentwickelte forensische Software, alles nur um Daten nicht zu verlieren oder sie wieder herzustellen. Bei diversen Firmen sitzen Techniker in Reinräumen und puzzeln Festplattenteile zusammen, um die darauf befindlichen Daten wieder nutzbar zu machen. Viel Aufwand, um keine Daten zu verlieren, aber wie wird man Daten sicher wieder los? Was mit Daten machen, die nun wirklich verschwinden sollen? Das sind Fragen, mit denen sich die unterschiedlichsten Interessensgruppen befassen: IT-Forensiker, Datenschützer und nicht zuletzt die Cyber-Kriminellen.

Fragen über Fragen...

Auch bei der Vernichtung von Daten steht der IT-Verantwortliche wie immer vor einem Berg von Fragen:

- Wo im Unternehmen befinden sich digitale Daten?
  Im Server, auf den PCs, im Drucker, in den Handys, auf CDs, DVDs, Bändern, Kameras, iPods… fast wären die Daten auf USB-Sticks vergessen worden und wenn man genau schaut, noch an vielen anderen Stellen.
- Wie sensibel sind die Daten?
  Hilfreich ist dazu ein Blick in die DIN 32757 und ihre 5 Sicherheitsstufen: allgemeines Schriftgut, das unlesbar gemacht werden soll, interne Unterlagen (u.a. Fehlkopien), personenbezogene Daten, geheimes essentiell wichtiges Schriftgut oder gar Daten, die einer besonderen Geheimhaltung unterliegen.
- Was soll mit den Datenträgern passieren?
  Können die Datenträger komplett zerstört werden oder sollen nur die Daten darauf verschwinden, damit die Datenträger einem anderen Zweck zugeführt werden können (Stichwort (Online-)Auktionen).
- Sind Fristen zu wahren?
  Für die Aufbewahrungsfristen gibt es die unterschiedlichsten Vorschriften, u.a, das Handelsgesetzbuch §238 und §257 und die Abgabenordnung §147, aber auch viele Vorschriften für spezielle Daten, wie Krankenakten oder die Betriebserlaubnis für Kernkraftwerke.

Do-it-yourself oder doch den Profi machen lassen?

Neben dem Kosten-/Nutzen-Faktor, der Wichtigkeit der Daten und dem weiteren Verwendungszweck der Datenträger steht auch die Vertrauenswürdigkeit des Datenvernichtungsunternehmens im Blickpunkt. Der Datenschutzbeauftragte sollte auf jeden Fall ein Audit bei dem in Frage kommenden Unternehmen durchführen um sicher gehen zu können, dass die Daten, die dort zur Vernichtung abgegeben werden, auch korrekt vernichtet werden und nicht im Hobbykeller des Einzelunternehmers in der Mirkowelle verschwinden.
Auf jeden Fall aber, egal, ob die Daten außer Haus oder innerbetrieblich vernichtet werden, sollte den Mitarbeitern bewusst sein, welche Datenträger im Umlauf sind und welche Daten sie enthalten. Idealerweise gibt es dazu eine betriebliche Richtlinie und regelmäßige Schulungen, denn die meisten Datenpannen passieren, wenn ein Notfall eintritt. In Stresssituationen werden gerne Geräte mit samt den Festplatten an die Support-Firma übergeben, nur um schnell wieder arbeiten zu können, ohne an die Vertraulichkeit der Daten zu denken.

Löschung schon vor dem Speichern planen
Was wie ein Paradoxon klingt, kann durchaus hilfreich sein. Wenn vor der Ablage der Daten auch ein Entsorgungskonzept geplant wird, werden Datenpannen im Stressfall vermieden. Hilfreich sind unter Umständen die Implementierung eines RAID 5 mit mehr als 3 aktiven Datenplatten, denn aus einzelnen Platten können kaum Daten rekonstruiert werden, besonders, wenn die Strategie mit einer Verschlüsselung kombiniert wird. Auch die Klassifizierung von Daten kann hilfreich sein, denn für Daten der Stufe 1 (allgemeine Unterlagen) muss deutlich weniger Aufwand getrieben werden, als bei geheimen Daten. Auch darf man sich aus Kostengründen nicht scheuen, auf die Garantie eines Datenträgers zu verzichten und ihn besser zu vernichten, als den Garantieanspruch wahr zu nehmen.

Datenvernichtung – die harte Tour
Werden die Datenträger nicht weiter verwendet, können sie komplett vernichtet werden. Dazu können mit Hilfe eines Degaussers die Festplatten mit einem starken Magnetfeld gelöscht, über die Currietemperatur erhitzt, die Oberfläche abgefräst werden oder die Magnetplatte in kleine Teile geschreddert werden (nicht zu große Teile machen, sonst können Daten eventuell rekonstruiert werden!). Optische Datenträger bedürfen lediglich einer Zerstörung der Oberfläche, während der Aufwand zur Zerstörung von USB-Datenträgern oft eine enorme physische Herausforderung werden kann.

Der Fachmann rät: drei bis sieben Mal überschreiben
Werden Datenträger der Stufe 1 und 2 weitergegeben oder müssen PCs an den Leasinggeber zurück gegeben werden, so sollte mittels Software der Datenträger drei bis sieben Mal überschrieben werden. Die dafür angebotene Software weißt sowohl preislich als auch qualitativ große Unterschiede auf. Auch das Einsatzgebiet kann enorm differieren, denn Datenvernichtung auf USB-Sticks unterliegt anderen Kriterien als permanente Datenlöschung über das Netzwerk.

Allgemeine Hinweise zur Datenvernichtung
(1) Im Zweifelsfall, ob die Daten sensibel sind oder nicht, sollte immer eine komplette Zerstörung der Datenträger vorgezogen werden
(2) Defekte Datenträger immer vor der Rückgabe komplett zerstören (dies ist aber mit dem Anbieter vorab zu vereinbaren) oder auf die Garantieleistung verzichten
(3) Müssen Datenträger zu Service- oder Reparaturzwecken das Haus verlassen, sollte ein Vertrag zur Geheimhaltung und Einhaltung des Datenschutzes geschlossen werden. Zur Not sollten Sie sich auch nicht vor einem Audit scheuen.
(4) Müssen Daten mittels Datenträger an Dritte übergeben werden, sollten Sie immer neue Datenträger verwenden.
(5) Dokumentieren der Datenlöschung und der Datenweitergabe, um den Compliance-Anforderungen zu genügen.