

IT-SECURITY

Löschen und was übrig bleibt

Jede Woche beantworten Sicherheitsexperten Leserfragen und geben Ratschläge, wie sich die Sicherheit in einem Unternehmen erhöhen lässt.

ILLUSTRATION: CW/THU



Frage: Wie funktioniert sicheres Löschen?

Ein Benutzer löscht seine Daten, indem er die entsprechende Datei in den Papierkorb zieht. Natürlich weiss er, dass die geheime Datei noch nicht futsch ist. Dies geschieht, sobald er den Papierkorb leert. In diesem Moment wird die Datei aus dem Index des Verzeichnisses entfernt, die entsprechenden Blöcke auf der Festplatte werden als «frei» markiert, worauf sich dort bei Gelegenheit neue Daten breit machen.

Solange diese Blöcke nicht überschrieben wurden, ist es möglich, die gelöschten Daten per Software zu rekonstruieren. Magnetische Datenspeicher lassen sich durch das Erstellen eines MFM-Bildes (magnetic force microscopy) rekonstruieren. Hierbei kann auch eine überschriebene Datei wieder hergestellt werden. Dies funktioniert, da der Schreibkopf nie eine gesamte Zone polarisiert, sondern nur den grössten Teil. So weist eine 0-Zone, welche durch eine 1 überschrieben wird, weniger Magnetismus auf als eine mit 1 überschriebene 1.

Um eine Software-basierende Datenrekonstruktion zu verhindern, muss eine Datei (bzw. deren Inhalt) genau ein-

mal komplett überschrieben werden. Das Pattern (Muster) ist irrelevant, oft werden jedoch Nullen (0x00) verwendet. Diese Löschmethode wird auch als «zero one pass» bezeichnet.

Die Rekonstruktion per MFM wird erschwert, indem jede Zone so oft wie möglich umgepolt wird. Der amerikanische Standard DoD.5200.22-M definiert

«Viele Wiping-Produkte auf Dateibasis ignorieren Codierung und Prüfsummen komplett und setzen die Algorithmen falsch um, was eine Rekonstruktion erleichtert.»

drei Schreibdurchgänge, wobei zuerst Nullen (0x00), Einsen (0xFF) und eine Zufallszahl geschrieben werden. Ein vierter Durchgang sollte die Zufallszahlen verifizieren.

Dieser Standard bietet nicht wesentlich mehr Schutz als «zero one pass». Diese wenigen Durchgänge aber werden aus Benutzersicht noch toleriert. Der Folgestandard DoD.5200.28-STD definiert bereits sieben Durchgänge, was eine gute Sicherheit für vertrauliche Informationen bietet.

Nach dem Deutschen VSITR-Standard des BSI wird eine Festplatte ebenfalls in sieben Durchgängen überschrieben, wobei

nach jedem Durchgang das Bitmuster des vorherigen umgekehrt wird. Der Vorgang wird mit 0x55 (01010101) abgeschlossen. Als sicherster Löschalgorithmus gilt derzeit der von Peter Guttmann, welcher allerdings 35 zeitintensive Schreibdurchgänge vorsieht.

Bei der Implementierung von Secure Wiping ist zu beachten,

lich. Um einen ungebetenen Datenretter abzuschrecken, bleibt das Entmagnetisieren oder das physische Schreddern. Beides erfordert Gerätschaften die sich nur wenige Unternehmen leisten wollen. Als beliebte und kostengünstigere Alternative mit therapeutischen Nebenwirkungen zückt da schon mal der Administrator die Bohrmaschine und übt Rache.

Datenerstörung kann zwar Spass machen, für ein paar Löcher im Zylinder wird ein erfahrener Spezialist aber nur ein müdes Lächeln aufbringen. Einen anderen Ansatz verfolgt die Festplattenverschlüsselung. Der Schlüssel sollte sich allerdings nicht auf der Platte befinden, wie es bei einigen Produkten der Fall ist. Er sollte sich auch nicht zu lange im Arbeitsspeichertumeln, denn auch das RAM kann sich an mehr erinnern, als es eigentlich sollte. ■



Der Autor
Simon Wepfer ist CTO bei der Sicherheitsberaterin Oneconsult, Thalwil.
www.oneconsult.com

Unsere Experten beantworten Ihre Fragen. Schreiben Sie uns: it-security@computerworld.ch

Ein Archiv der Helpdeskartikel finden Sie im Internet: www.computerworld.ch