Sicheres Löschen von Speichermedien

Blitzblank

Lukas Grunwald

Mit Betätigen der „Delete"-Taste sind Dateien noch längst nicht ins Nirwana entschwunden – dafür müssen professionelle Tools zum sicheren Datenlöschen her. Doch auf sie ist leider nur begrenzt Verlass, wie der *iX*-Vergleichstest ergab.

Bei einem Festplattencrash oder anderen Systemkatastrophen ist jeder Betroffene überglücklich, dass dank ausgefeilter Techniken und Werkzeuge von Datenrettungsfirmen ein Großteil der vermeintlich zerstörten Daten wiederhergestellt werden kann. An die Kehrseite der Medaille denkt allerdings kaum jemand: Mit Betätigen der Löschtaste sind Daten noch längst nicht vom Rechner verschwunden.

Unternehmen, die nicht mehr benötigte PCs verkaufen oder Leasing- und Leihgeräte nach geraumer Zeit wieder zurückgeben, sollten sich versichern, dass keine sensiblen Daten oder -spuren mehr auf der Festplatte zu finden sind. Auch wenn jemand beim Kauf eines neuen PC den alten in Zahlung gibt, kann vorheriges gründliches „Putzen" der Platte von Vorteil sein.

Eine Neuinstallation des Betriebssystems oder das Löschen einer Datei ist nur vermeintlich sicher: Da alle Filesysteme beim Löschvorgang lediglich den Directory-Eintrag entfernen, der auf den Speicherort der Datei verweist, bleiben die eigentlichen Informationen physikalisch erhalten. Selbst wenn der Datenträger formatiert oder einfach nur komplett mit Nullen überschrieben wird, bleibt mit dem Rest-Magnetismus – auch Remanenz genannt – immer noch ein Weg, an die Daten zu gelangen (siehe Kasten „Physikalische Datenvernichtung").

Letzteres gilt zumindest noch für Festplatten der älteren Generationen. Mit zunehmender Speicherdichte bei den neueren Platten steigt auch der Aufwand zur Wiederherstellung überschriebener Daten – Erfolgsgarantien gibt es jedoch keine. Im Test unserer Schwesterzeitschrift c't [1] gelang es mehreren Datenrettungslaboren nicht, mit Standardmitteln die Testdateien auf den mit Nullen überschriebenen Festplatten wiederherzustellen. Allerdings wurden nicht alle Mittel ausgeschöpft, ein Labor etwa verwies auf den „sehr großen technischen und finanziellen Aufwand" für weitere Untersuchungen.

Kein aktueller Standard

Auch in Expertenkreisen herrscht Uneinigkeit. Forensikspezialist Larry Leibrock von der University of Texas at Austin etwa ist davon überzeugt, dass viele der vermeintlich überschriebenen Daten wiederherstellbar sind. Der Sicherheitsexperte Peter Gutmann, der 1996 eine eigene Löschmethode vorstellte, räumt hingegen ein, dass die bekannten Löschalgorithmen speziell auf die älteren, heute obsoleten Speichertechniken zugeschnitten waren. Sicherheitshalber empfiehlt er jedoch auch heute noch: „A few passes of random scrubbing is the best you can do." Denn, so schrieb er an *iX*, „this was true in 1996, and is still true now".

Empfehlenswert ist auf alle Fälle, beim Löschvorgang den so genannten Schutzbedarf der zu entfernenden Daten angemessen zu berücksichtigen. Bis die Fachwelt ihre Erkenntnisse an aktuelle Speicherstandards angepasst hat und keine älteren Speicherplatten mehr in Benutzung sind, sollte man lieber eine Runde zu viel als zu wenig überschreiben, insbesondere wenn es sich um sensible Firmendaten handelt.

Dass unabhängig vom Alter der Festplatte und der Brisanz der Daten vielen Computerbenutzern die Problematik des Löschens nicht bekannt ist, zeigt ein kürzlich erfolgtes Expe-

iX-TRACT

- Das Betätigen der Delete-Taste löscht eine Datei nicht physisch, sondern lässt lediglich den Verweis auf sie im Directory verschwinden.
- Wer mit sensiblen digitalen Daten zu tun hat, sollte vor dem Ausmustern, Verkaufen oder jedwedem Weitergeben eines Rechners ordentlich die Festplatte „putzen".
- Wichtiger als die einfache Handhabung professioneller Löschtools ist das Überschreiben der freien Speicherbereiche, auf denen unter Umständen noch Daten-Altlasten liegen.
- Auf älteren Festplatten ist wegen der geringeren Speicherdichte die Datenrekonstruktion einfacher als auf modernen Medien.

riment: Ein Forscherteam des Massachusetts Institute of Technology (MIT, web.mit.edu) erwarb bei eBay und verschiedenen Gebrauchtwarengeschäften 158 Festplatten, von denen lediglich 12 frei von Datenspuren waren [2]. Auf den anderen konnten die Forscher mit Hilfe forensischer Tools medizinische Daten, Pornografie, Liebesbriefe, Kreditkartennummern und weitere sensible Informationen rekonstruieren. Höhepunkt war der Fund einer Festplatte, die allem Anschein nach einst Bestandteil eines Geldautomaten war: Auf ihr fanden sich Kontonummern, Kontostände, Zugangsdaten und Teile der Automatensoftware.

Und Ende März forderte die Datenschutzbeauftragte des Landes Nordrhein-Westfalen, Bettina Sokol, Behörden zum sicheren Löschen ihrer Daten vor der Ausmusterung ihrer Rechner auf. Anlass der mahnenden Worte war der Fund sensibler personenbezogener Daten auf einem gebrauchten PC, den der Käufer dem Landesdatenschutzzentrum gemeldet hatte. Die Datenschutzbeauftragte verwies auf die Existenz spezieller Löschtools.

Diese Softwarewerkzeuge sind quasi als Abfallprodukte der forensichen Analyse und der Datenrettung entstanden. Das Vorgehen ist bei allen Tools gleich: Sie versuchen, auf dem physikalischen Sektor die Daten mit bis zu 35 speziellen Pattern (Bitmuster) so zu überschreiben, dass alle Kodierungen ausgenutzt werden und aus dem entstandenen Restmagnetismus keine brauchbaren Dateifetzen mehr zu rekonstruieren sind.

Grundsätzlich existieren zwei verschiedene Arten von Softwarewerkzeugen. Eine der beiden ist für das Löschen einzelner Dateien im Filesystem konzipiert. Sie ist als Dienstprogramm (bei Unix, GNU/Linux und Win32) oder Shell-Erweiterung in Windows-Betriebssystem integriert. Wenn nun eine Datei zu löschen ist, wird sie nicht umbenannt oder ihr Eintrag aus dem Directory entfernt, vielmehr überschreibt das Werkzeug sie mehrfach mit Löschpattern und löscht sie anschließend.

Ein Löschtool sollte außer den explizit zum Löschen bestimmten Daten auch alle freien Bereiche des Speichers überschreiben. Unter Umständen befinden sich dort noch „Altlasten" in Form von Daten, deren Verweise vor der Installation des Tools durch Betätigen des Delete-Buttons entfernt wurden.

Je nach Anbindung und Filesystem kann das Löschen auch per Fernzugriff (Remote) auf Servern erfolgen – Erfolgsgarantie gibt es jedoch keine. Ist etwa ein Versionskontrollwerkzeug dazwischen geschaltet, klappt das Löschen nicht.

Löschen durch Überschreiben

Die zweite Kategorie von Tools löscht die komplette Festplatte oder Partition. Dazu bootet man meistens von einer Diskette oder CD aus und greift über einen Systemtreiber direkt auf das Speichermedium zu. Oft liefern die Hersteller für diesen Zweck ein eigenes Betriebssystem auf einer Bootdiskette mit – ausgesprochen beliebt ist Caldera DR-DOS.

Zum Testen kam ein 500 MHz schneller Pentium III mit einem Adaptec 2940U2W und einem von Intel in den BX 340 (onboard) integrierten IDE-Controller zum Einsatz. Schwerpunkte des Tests waren Benutzerfreundlichkeit und Handhabbarkeit des Werkzeugs sowie die Zuverlässigkeit des Löschvorgangs. Jedes Tool musste sich an zwei Festplatten – IBM DCAS-3433OW und

Seagate ST-3144A – versuchen. Die beiden Platten wurden mit Suchmustern präpariert, die in Form von Dateien und einer direkten Markierung auf Sektorbasis angebracht wurden. Nach dem Löschen suchte ein Forensik-Toolkit nach diesen Markierungen, die bei einem gelungenen Löschvorgang vollständig entfernt sein müssten.

Ibas Expert Eraser

Der Expert Eraser von Ibas, der wie die folgenden drei Tools zu den reinen Festplatten-Cleanern gehört, wird auf einer bootbaren Diskette ausgeliefert.

Leider funktionierte das Erkennen des Adaptec-Controllers nicht auf Anhieb. Erst nachdem per Hand der ASPI-Treiber auf der Diskette installiert wurde, war der Eraser in der Lage, auch SCSI-Festplatten blank zu putzen.

Von den anfänglichen Erkennungsschwierigkeiten einmal abgesehen, konnte das Tool alle Festplatten zuverlässig und sicher löschen.

Kroll Ontrack DataEraser

Kroll Ontrack liefert 2 Disketten aus, darunter eine bootbare mit dem Betriebssystem DR-DOS 7.03. Der automatische Erkennungsmechanismus (Autodetect) des Betriebssystems erkannte leider den Adpatec 2940U2W nicht, sodass nur die IDE-Festplatte gelöscht werden konnte. Die Seagate-Festplatte war außerdem nicht vollständig und gründlich gelöscht, die forensische Untersuchung ergab, dass die Pattern ab Adresse 0x07c8600 unverändert auf der Festplatte verblieben waren.

Nach einem Support-Call schickte Kroll Ontrack umgehend eine neue Softwareversion, die nun auch ohne Schwierigkeiten mit dem Adaptec-SCSI-Hostadapter zusammenarbeitete und in der Lage war, die SCSI-4-GByte-HD vollständig zu löschen. Mit der Seagate-Festplatte hatte allerdings auch diese Version wenig Erfolg: Noch immer befanden sich Datenreste auf der Platte.

Ein erneuter Supportanruf ergab, dass so „alte“ Festplatten nicht mehr unterstützt würden und die Minimalanforderung für das Funktionieren des Produktes somit nicht erfüllt seien. Eine Nachbesserung wäre hier schon deswegen empfehlenswert, weil speziell im kommerziellen Umfeld häufig noch ältere PCs und Festplatten eingesetzt werden.

Löschen nach Norm

Es gibt mehrere anerkannte Methoden, wie man ein Speichermedium sicher löschen kann.

Single-Pass: Dabei werden die Daten einfach mit einer „1“ oder einer „0“ auf Bitebene überschrieben. Mit einem Pattern-Analyzer lässt sich allerdings das Komplement der Daten bilden, und die Orginaldaten können unter Umständen wie bei einem Fotonegativ wieder sichtbar gemacht werden. Solche Geräte existieren in manchen Datenrettungslaboren.

DoD 5220.22-M: Verfahren des US-Department of Defence. Die Originaldaten werden durch dreifaches Überschreiben nach den Bestimmungen NTSC-TG-025 (Version 2, Sept. 1991) des US-amerikanischen Verteidigungsministeriums vernichtet. Die Festplattendaten werden hierbei zunächst mit einem fest vorgegebenen Bitmuster und anschließend mit Pseudozufallszahlen überschrieben. Das Überschreiben in der dritten Runde erfolgt mit komplementären Werten der Runde 1.

NISPOM (NSA DoD 5220.22-M ECE): Die National Security Agency empfiehlt, das DoD-5220.22-M-Verfahren einmal anzuwenden, dann Zufallsdaten zu schreiben, und erneut das DoD-5220.22-M-Verfahren zu benutzen.

BSI-Empfehlungen: Das Bundesamt für Sicherheit in der Informationstechnik empfiehlt mindestens zweimaliges, besser dreimaliges Überschreiben mit nicht gleichförmigen Mustern.

NAVSO P-5239-26 (RLL, MFM): Löschvorschrift des Navy Aviation Supply Office, die je nach Aufzeichnungsformat ein anderes Überschreibmuster und eine bestimmte Rundenzahl vorsieht.

Peter Gutmann: Die in dem 1996 gehaltenen Vortrag „Secure Deletion of Data from Magnetic and Solid-State Memory“ beschriebene Methode des australischen Sicherheitsexperten Peter Gutmann gilt als die sicherste. Nach ihr sollen Daten in 35 Durchgängen abwechselnd mit speziellen Bitmustern und Zufallsdaten überschrieben werden. Das Besondere daran ist, dass sich diese Methode ebenfalls dazu eignet, nicht flüchtige Speicherbausteine zu löschen.

Bruce Schneier: Der bekannte Kryptologe Bruce Schneier entwickelte einen Algorithmus, der in sieben Durchläufen für das sichere Überschreiben der Daten sorgen soll.

Orange C-II Shred ist das hauseigene Verfahren der Firma Convar. Dabei wird jeder Sektor sechsmal hintereinander mit einem High-/Low-Signal unter Verwendung eines speziellen Kalibrierverfahrens überschrieben. Sinn und Zweck der Übung soll das Überschreiben der so genannten Randbereiche der Spuren sein.

Positiv zu bewerten ist hingegen das übersichtliche Menü, das es ermöglicht, sich die Sektoren direkt anzusehen, um das Löschen einzelner Bereiche nachvollziehen zu können. Des Weiteren lässt sich im Programm die Menge der Überschreibzyklen beliebig einstellen.

Blancco Data Cleaner

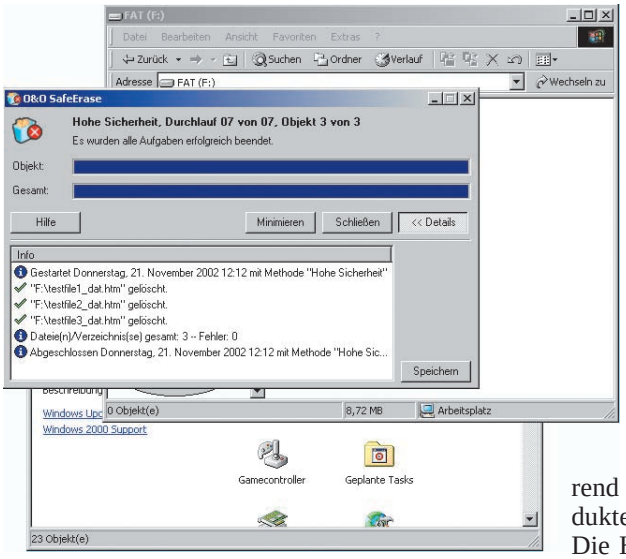
Ebenfalls auf einer Diskette liefert Blancco seinen Data Cleaner aus, der offenbar auf einem GNU/Linux-System basiert. Das Unternehmen hat für das Löschwerkzeug ein auf der SVGA Lib basierendes Frontend entwickelt, das eigentliche Funktionieren verdankt der Data Cleaner den bekannten GNU-Tools *sfdisk* und *mkdosfs*, die sich in einer Initial Ramdisc befinden. In ihrer jetzigen Formulierung verstoßen die Lizenzbestimmungen des Produkts gegen die GNU Public Licence (GPL). Der Hersteller verspricht, bei der nächsten Version nachzubessern.

Nach dem Anwählen der zu löschenden Festplatte im Menü startet das Programm. Langsam, aber gründlich könnte die Devise für den Data Cleaner lauten, denn immerhin dauerten drei Durchläufe – die mittlere der voreingestellten Optionen – bei einer 130,7 MByte großen Atapi-Harddisk mehr als eine Stunde. Danach war die Platte aber auch zu 100 % gelöscht.

Convar PC Inspector Disk Erasing

Über den Webshop bietet Convar die PC Inspector Disk Erasing Software an. Dort ist eine kostenlose Version zum Download verfügbar. Wer jedoch seine Daten mit einem annehmbaren Sicherheitsniveau löschen möchte, sollte besser die Pro-Version durch einen Kauf eines Freischaltcodes erwerben. Um die Festplatte „ordentlich“ zu reinigen, steht der hauseigene Orange C-II Shred-Algorithmus zur Verfügung.

Obwohl das Programm für die Betriebssysteme Windows 98, ME, 2000 und XP sein soll, war es nicht in der Lage, unter Ersterem eine der Testfestplatten zu löschen. Unter Windows 2000 lief es jedoch ohne Schwierigkei-



Nach getaner Arbeit liefert SafeErase ein Löschprotokoll für die Akten – oder für den Chef (Abb. 1).

ten. Nach der forensischen Analyse des Löschergebnisses war allerdings festzustellen, dass der PC Inspector an der 130-MB-AT-Bus-Festplatte scheiterte: Die Endbereiche der Platte hatte er nicht überschrieben.

Die Software ist derzeit nicht mehr erhältlich, ein neues Löschtool namens e-maxx ist jedoch in Vorbereitung. Das ab Mai 2003 kostenlos zur Verfügung stehende Werkzeug wird auf Linux basieren und als Bootdiskettenversion ausgeliefert.

Acronis DriveCleanser

Bei der Installation des Softwarepakets DriveCleanser erstellt das Setup-Programm eine Löschdiskette, die die gesamte Festplatte löschen kann.

Dazu sind allerdings erst einmal drei Bootdisketten zu erstellen, während bei den Konkurrenzprodukten eine einzige ausreicht. Die Handhabung ist somit ungleich umständlicher. Umso mehr, da die Software nach dem Beispielen der drei angekündigten Disketten unerwartet nach einer vierten verlangt. Ein Telefonat mit dem Support ergab, dass man bei Vorhandensein eines CD-Brenners im Rechner auch eine bootbare CD erstellen kann. Das funktionierte reibungslos.

Der DriveCleanser setzt auf Linux auf. Mit dem optisch an Windows XP angelehnten Programm, das auf dem FOX-Toolkit basiert und daher vier Disketten in Beschlag nimmt, hat auch der unerfahrene Benutzer eine Chance. Alle wichtigen Algorithmen vom DoD 5220.22-M über NAVSO bis hin zu Peter Gutmann (siehe Kasten „Löschen nach Norm“) stehen zur Verfügung, und an den gelöschten Festplatten war nichts zu beanstanden. Besonders erwähnenswert ist die Tatsache,

Physikalische Datenvernichtung

Um das Risiko zu umgehen, dass eine Softwarelösung ihren Dienst versagt, können besonders misstrauische Menschen ihre Daten physikalisch vernichten.

Entmagnetisieren

Medien, die Daten mittels lokaler Magnetisierung speichern, lassen sich mit einem „De-Gausser“ entmagnetisieren. Die Einheit Gauss für die magnetische Flussdichte wurde im SI durch Tesla abgelöst (1 Gauss entspricht 0,0001 Tesla).

Ein solches Gerät, das ähnlich auch in vielen Röhrenmonitoren zu finden ist, setzt die Platte oder das Band einem magnetischem Wechselfeld abnehmender Amplitude aus.

Beim Abschalten eines externen Magnetfelds bleibt die magnetische Ausrichtung teilweise erhalten (Remanenz) und damit die Information auf dem Datenträger. Um diese Magnetisierung zu entfernen, ist ein Gegenfeld der „Koerzitivfeldstärke“ erforderlich. Im angelsächsischen Raum ist für die magnetische Feldstärke bis heute die Einheit Oersted gebräuchlich, die im SI rund 79,6 Ampere/Meter entspricht. Die anfängliche Koerzitivfeldstärke, um die Informationen sicher zu löschen, ist vom Datenträger und seinem magnetisierbaren Material abhängig.

Alternativ kann der Datenträger über den Curie-Punkt (Temperatur, bei der ein Material seine ferromagnetischen Eigenschaften verliert) erhitzt werden, bei reinem Eisen (Fe) sind das über 750 °C. Danach sind die Informationen auch vollständig und sicher gelöscht. Doch selbst wenn ein Festplattengehäuse vorübergehend solcher Hitze ausgesetzt ist, etwa bei einem Brand, lassen sich bisweilen alle Daten retten, da sich solche Temperaturen nur bei langer Hitzeeinwirkung direkt auf den Plattenoberflächen erreichen lassen.

Schreddern optischer Datenträger

Da CD-Rs resistent gegenüber Magnetfeldern sind, erfordern sie eine mechanische Vernichtung. Einer zu Granulat zermahlenen CD-R läßt sich kaum jemals wieder Daten entlocken. (un)

DATEN- UND FESTPLATTENLÖSCHWERKZEUGE

Hersteller	Acronis	AKS-Labs	Blancco Ltd.	Convar Deutschland GmbH	CyberScrub LLC
Produkt	DriveCleanser 6.0	QuickWiper	Data Cleaner 3.2	PC Inspector Disc Cleaning	CyberScrub 2.0
URL	www.acronis.com	www.quickwiper.com	www.blancco.com	www.pcinspector.de/	www.cyberscrub.com
Betriebssystem	Windows ab 95	Win2k, XP	Linux	Win2k, XP	Win2k, XP
Preis	49,95 €	29,95 US-$	24,95 €	k. A.	CD 59,95 US-$, Download 49,95 US-$
Ohne Betriebssystem benutzbar	Floppy, CD-R		Floppy		
Löschen von					
kompletten Festplatten	✓	✓	✓	✓	
Partitionen	✓		✓		
Dateien		✓			✓
unbenutzten Filesystembereichen		✓	✓		✓ (schlecht implement.)
SCSI-Adaptec 2940U2W mit IBM DCAS-4.3 GB	✓	✓	✓	✓	✓
ATA-Interface mit Seagate 130 AT-BUS HD	✓	✓	✓	–	✓
unterstützte Löschalgorithmen					
DoD	✓	✓			
NISPOM		✓			
Gutmann	✓				
andere/eigene	✓		✓	✓	✓
Bemerkungen	Ergebnisüberprüfung in Viewer	neue deutsche Version gerade erschienen	Löschprotokoll	neues Tool in Vorbereitung	Version 3 gerade erschienen

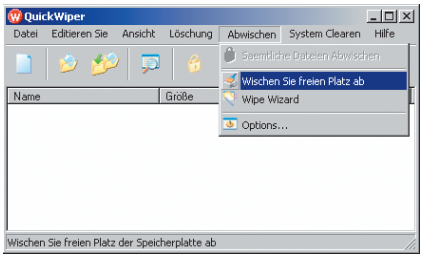
✓ vorhanden bzw. funktioniert – nicht vorhanden bzw. funktioniert nicht k. A. keine Angabe

dass der Acronis DriveCleanser auch USB- und Firewire-Festplatten löschen kann und somit ebenfalls Tokenspeicher, die oft zum Ablegen von geheimen Schlüsseln und anderen wichtigen Daten benutzt werden.

Wipe

Wipe ist ein frei verfügbares Tool, das unter verschiedenen Linux- und UNIX-Betriebssystemen Dateien und ganze Filesysteme sicher löschen kann. Die Software ist mit Signaturen gegen Manipulation gesichert.

Das Werkzeug basiert auf dem Löschalgorithmus von Peter Gutmann und ist damit sowohl für Flash-Speicher als auch für magnetische Aufzeichnungsmedien geeignet. Ein Besonderheit ist die Möglichkeit zum Löschen von Bändern, was allerdings das Bandlaufwerk stark strapaziert.



Im Test befand sich noch die "Babelfisch"-Variante des QuickWiper, die just erschienene Version ist sprachlich überarbeitet (Abb. 2).

Leider kann Wipe nicht die leeren Bereiche eines Filesystems löschen. Das Löschen ganzer Festplatten und Dateisysteme erledigt das Tool dafür ausgesprochen zuverlässig.

CyberScrub

Nach der einfachen Installation von CyberScrub des gleichnamigen Herstellers lässt sich unter den vorhandenen Löschmethoden die gewünschte auswählen: nicht mehr Software- oder Hardware-Recoverable, als dritte Alternative lässt sich aus Vorgaben ein eigener Algorithmus zusammenstellen.

Um die leeren Bereiche zu löschen, erzeugt CyberScrub eine Datei, die den Plattenplatz belegen soll, und löscht nicht direkt die Blöcke im Filesystem. Bei virtuellen Speicherkapazitäten mit dynamischer Ressourcenzuweisung funktioniert diese Methode allerdings nicht mehr.

Von dieser Schwäche abgesehen arbeitet das Programm einwandfrei, die Analyse ergab keine Überreste von Daten. Um das Sicherheitsniveau anzuheben, verfügt das Tool über einige spezielle Features. So kann CyberScrub einen Registry-Eintrag setzen, der beim Herunterfahren des Rechners die Page- und Swap-Bereiche überschreibt und somit Spuren und Daten vernichtet.

Um Filesystemobjekte zu löschen, muss der Anwender sie via Drag & Drop auf den neuen schwarzen Eimer mit dem Strahlensymbol ziehen. Alternativ kann er die so genannte Erase-beyond-recovery-Methode beim Leeren des Papierkorbes auswählen. Das Löschen der Daten ist nicht über ein Kontextmenü möglich.

O&O SafeErase

SafeErase von O&O Software lässt sich ausgesprochen einfach installieren. Nachdem die Software registriert ist, integriert sie sich als Shell-Erweiterung vollkommen in das Windows-Betriebssystem. Mit SafeErase lassen sich Dateien sowohl über den Papierkorb als auch direkt über das Kontextmenü sicher entsorgen. Über einen Schieber kann man den Löschalgorithmus – von Peter Gutmann über NSA, NISPOM, BSI und DoD – einstellen. Als eines der wenigen Programme kann SafeErase Löschprotokolle erstellen (Abb. 1). Die Arbeit wird zuverlässig durchgeführt, die Analyse ergibt keinerlei Reste der Testdateien nach dem Löschen im Filesystem.

Leider unterstützt O&O nicht die Option, freie Festplattenbereiche zu löschen. Somit lassen sich zwar aktuell

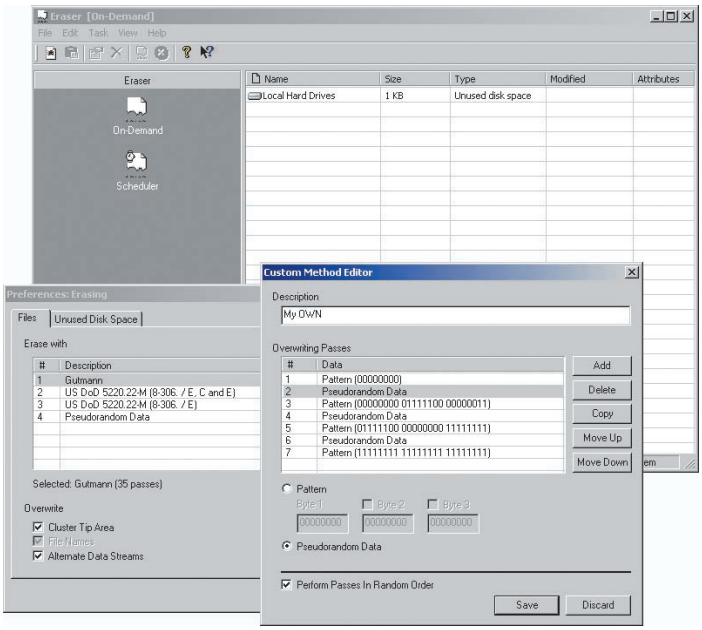
Ibas Deutsch-land GmbH	Jetico Inc.	Kroll Ontrack GmbH	O&O Software GmbH	Sami Tolvanen	
Expert Eraser	BestCrypt Wipe	DataEraser	SafeErase	Eraser 5.3	WIPE 2.1.0
www.datenloeschung.de	www.jetico.com	www.ontrack.de/dataeraser/	www.oosoft.de	www.tolvanen.com/eraser/	wipe.sourceforge.net/
Caldera DOS	Win2k, XP, Linux, Unix	DR-DOS 7.03	NT 4, Win2k, XP	Windows 2K, XP	Linux, UNIX
1 Löschlizenz 28,00 €	1 Löschlizenz 39,95 US-$	358,00 €	49,00 €	Freie Software/GPL	Freie Software/GPL
Floppy		Floppy			
✓		✓			✓
		✓			✓
	✓		✓	✓	✓
	✓ (nur unter Windows)			✓	
✓	✓	✓ (nach Update)	✓	✓	✓
✓	✓	–	✓	✓	✓
✓	✓	✓	✓	✓	
			✓		
	✓		✓	✓	✓
✓	✓	✓	✓	✓	
Löschprotokoll; versch. Levels	löscht Swap-Bereich im Betrieb	Löschprotokoll	Löschprotokol/erw. Version BlueCon XXL erschienen	zeitgesteuertes Löschen freier Festplatten-bereiche	

vorhandene Dateien sauber löschen, nicht aber diejenigen, die sich vor der Installation von O&O SafeErase auf dem Datenträger befanden oder die über eine Systemfunktion entfernt wurden.

So entfernt SafeErase auf Wunsch des Anwenders zwar das Original-Word-Dokument, das Backup, das Word automatisch beim Öffnen der Datei anlegt, ist auf diese Weise aber nicht vom System zu bekommen. In der Administrationssoftware O&O BlueCon XXL, die in der Zwischenzeit erschienen ist, ist nach Aussagen des Herstellers dieses wichtige Feature integriert.

AKS-Labs QuickWiper

Nach der Installation von QuickWiper (Abb. 2) steht ebenfalls auf dem Desktop eine neue virtuelle Mülltonne zur Verfügung. Die Handhabung ist allerdings sehr umständlich, da zum Löschen der Dateien immer erst der QuickWiper zu starten ist, beziehungsweise der Anwender die Dateien zum endgültigen Entsorgen mehrfach im Programm umherschieben muss: Erst muss er sie aus dem Systempapierkorb wiederherstellen, um sie anschließend mit QuickWiper explizit löschen zu



Mit dem finnischen Eraser kann sich jeder noch so misstrauische Anwender einen supersicheren Algorithmus zusammenklöppeln (Abb. 3).

können. Zudem wird bei jedem Benutzen der QuickWiper-Tonne eine Instanz des Programms gestartet.

Nach dem Löschen und dem sofortigen Ausschalten des Testrechners ließen sich die Inhalte der Testdateien aus den FAT-formatierten Datenträgern vollständig rekonstruieren. Die Dateien waren lediglich in den System-Papierkorb von Windows 2000 verschoben. Die NTFS-Volumes waren jedoch sauber mit Zufallswerten überschrieben. Vermutlich hat der Programmautor nicht sichergestellt, dass alle Dateien zuverlässig auf dem Datenträger landen.

Eraser von Sami Tolvanen

Den Eraser stellt der finnische Programmierer Tolvanen unter der GPL übers Web zur Verfügung. Die Binaries sind per PGP Key signiert, damit eine Manipulation der Daten auszuschließen ist. Ebenso ist der (signierte) Quellcode von der Webpage downloadbar.

Das Löschprogramm unterstützte alle gängigen Methoden von Gutmann bis zum US-Standard DoD 5220.22-M, enthält aber auch eigene Pattern und Pseudorandom-Daten. Wem das noch nicht reicht, der kann sich beliebige Löschmuster zusammenklicken (Abb. 3).

Über eine Shell-Erweiterung kann man sowohl Dateien auf direktem Weg löschen als auch den Inhalt des Papierkorbs. Die Analyse des Forensic-Images ergab, dass der Eraser nur Datenmüll hinterlässt. Über ein Steuerungsprogramm lassen sich die leeren Bereiche von Festplatten löschen, beziehungsweise kann man darüber das periodisches Löschen von Verzeichnissen oder Dateien automatisch ausführen lassen.

Wer vor Kommandozeilenbedienung nicht zurückschreckt, findet im Eraser ein zuverlässiges Löschtool mit vielen brauchbaren Extra-Features.

Jetico BestCrypt Wipe

Krypto-Hersteller Jetico liefert sein Löschtool BestCrypt Wipe für Unix im Quelltext und kostenlos aus, für die installierbare Windows-Software muss eine Lizenz erworben werden. Als Algorithmus kann der Anwender zwischen Peter Gutmann oder DoD 5200.28-STD wählen. Dabei ist den Programmierern in der Benennung offenbar ein Fehler unterlaufen, da die DoD 5200.28-STD-Publikation eine Kriteriensammlung für die Evaluierung von Computersystemen und kein Löschmechanismus ist. Das Löschen von freien Bereichen wird via Task-Scheduler zeitgesteuert erledigt, das einzelner Dateien über eine Erweiterung im Kontextmenü.

Die Unix-Version löscht keine freien Bereiche, sondern lediglich Dateien, das allerdings recht zuverlässig. Zusätzlich reinigt BC Wipe als einziges der getesteten Produkte im laufenden Betrieb den Swap-Bereich, was wohl auf die Erfahrung des Herstellers mit Krypto-Systemen zurückzuführen ist.

Zwei weitere Tools mussten zwar aus dem Test ausscheiden, sollen aber nicht unterschlagen werden: Secure HD Eraser des dänischen Programmierers Ole Tange verweigerte den Start mit Kernel-Panic. Und McAfees Quick Clean erwies sich nach mehreren vergeblichen Startversuchen und Supporttelefonaten als inkompatibel mit der Testumgebung.

Fazit

Das passende Tool sollte jeder Benutzer entsprechend des Schutzbedarfs seiner Daten und weiterer Erfordernisse auswählen. Für den Hausgebrauch genügt oft ein niedrigeres Sicherheitslevel, wie es sich beispielsweise beim Ibas Eraser oder Blancco Datacleaner einstellen lässt. Für professionelle Anwender kann etwa das Erstellen eines Löschprotokolls zu Nachweiszwecken (O&O-Tool und andere) oder das Löschen von Flash-Speichern mit sensiblen Firmendaten (Acronis DriveCleanser oder Wipe) relevant sein.

Wie sicherheitsrelevante Software über das Internet zur Verfügung gestellt werden sollte – mit Quelltext und Signaturen zum Überprüfen der Echtheit der Binaries –, zeigen lediglich zwei der getesteten Kandidaten, Tolvanens Eraser und das Linux-Tool Wipe.

Für welches Tool auch immer sich jemand entscheidet, jeder Versuch, Daten „richtig“ zu löschen, ist sicherer und besser, als nichts zu unternehmen. (ur)

LUKAS GRUNWALD

ist Consultant bei DN Systems, Hildesheim.

Literatur

[1] Lars Bremer, Axel Vahldick; Auf Nimmerwiedersehen; Dateien richtig löschen; c’t 5/2003, S. 192

[2] Simson Garfinkel, Abi Shelat; Remembrance of Data Passed: A Study of Disk Sanitization Practices; www.computer.org/security/v1n1/garfinkel.htm

[2] Peter Gutmann; Secure Deletion of Data from Magnetic and Solid-State Memory; www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html

[3] Heinrich Frohne; Elektrische und magnetische Felder; ISBN 3-519-40002-2

[4] Waldemar von Münch; Werkstoffe der Elektrotechnik; ISBN 3-519-10115-7