Acronis DriveCleanser
Benutzerhandbuch

Acronis
Compute with confidence
www.acronis.de

ACR07.ADC6-07.16

Inhaltsverzeichnis

Kapitel 1 Einführung

Müssen Sie einen alten PC loswerden, eine neue Festplatte einbauen, einen geleasten Computer zurückgeben oder eine Firmen-Leihstellung auflösen? In all diesen Fällen ist es notwendig, die auf den Datenträgern enthaltenen Daten komplett zu zerstören

Acronis DriveCleanser garantiert die komplette Zerstörung aller Daten auf ausgewählten Partitionen bzw. allen Datenträgern mit einer einfachen Benutzeroberfläche im Look von Windows XP und gezielten Aktionen.

Vertrauliche Informationen auf Festplatten: Speicherung und Zugriff

Heutzutage werden immer mehr vertrauliche Informationen in digitaler Form erstellt und auf Computern gespeichert. Auch die Mehrzahl aller Dokumente, die früher mit Schreibmaschinen oder andern Mitteln manuell erstellt wurden, ist heute auf Datenträgern gespeichert.

Es sind viele vertrauliche Daten auf Festplatten gespeichert, auch solch wichtige Dinge wie Bankdaten und Zugriffscodes, Kreditkartennummern, Geschäftsvorfällen, Bankbewegungen, Buchführungsdaten und Betriebsdaten. Es ist nicht möglich, alle **vertraulichen Daten** aufzuzählen, die unter keinen Umständen in fremde Hände geraten sollten.

Zerstörung vertraulicher Daten

Aus dem bisher geschriebenen ist zu ersehen, dass nicht nur für die Erstellung und Speicherung vertraulicher Daten sondern auch für deren Vernichtung spezielle Regeln gelten müssen.

Computer werden im Laufe ihres Lebenszyklus mehrere Male aufgerüstet und verändert. Vor allem die Speichermedien werden dabei oft vergrößert: anstelle kleinerer Platten kommen Festplatten mit mehr Speicherkapazität in das System. Wenn eine solche Festplatte eingebaut wird, dann werden die Daten der alten Platte oft auf die neue Platte übertragen und danach gelöscht. Genauso oft aber verbleiben die ursprünglichen Daten auf der alten Platte.

Die nachlässige Aufbewahrung der nicht mehr benötigten Festplatten kann zum Verlust vertraulicher Informationen führen. Der einzige sichere

Schutz vor dem Missbrauch vertraulicher Daten ist die komplette **Zerstörung** der Daten auf der alten Festplatte, wenn diese nicht länger benötigt wird bzw. die Daten auf die neue Festplatte transferiert wurden. Dabei liegt die Betonung auf **Zerstörung**! Gemeint ist in diesem Zusammenhang nicht etwa nur das einfache Löschen, sondern die tatsächliche unwiederbringliche Zerstörung der vertraulichen Daten. Der Unterschied zwischen diesen beiden Methoden wird an anderer Stelle beschrieben.

Der folgende Fall soll die Problematik verdeutlichen: Jack V., ein EDV Berater aus Brighton, erwarb bei der Auflösung einer Internetfirma einen gebrauchten Computer für 400 Dollar. Beim Einschalten wurden die sensiblen Daten der Firma sichtbar: Sozialversicherungsnummern, Löhne und Gehälter von 46 Angestellten, Auszahlungslisten, Firmenstrategien, vertrauliche Protokolle von Vorstandsversammlungen und anderen interne Dokumenten.

Das war nur ein Computer, die Firma hatte mehrere dieser Computer ausgesondert und verkauft.

Datenvernichtung mit Hilfe eines Betriebssystems

Es existiert ein bedeutender Unterschied zwischen dem Löschmechanismus eines Betriebssystems und einer speziell dafür entwickelten Software.

Der Hauptaspekt besteht darin, dass das Betriebssystem, wie z.B. Windows, die Informationen einer Datei nicht vollständig von der Festplatte löscht. Stattdessen wird der Name der gelöschten Datei, die sich in der Dateizuweisungstabelle (FAT) befindet, mit einem besonderen Zeichen versehen. Die angeblich gelöschte Datei wird für den User lediglich unsichtbar. Die Cluster, die die Datei eigentlich enthalten, werden als „frei“ betrachtet. Der eigentliche Inhalt und sogar fast der komplette Dateiname bleiben bis auf weiteres aber noch rekonstruierbar auf dem Datenträger erhalten. Somit ist es ein Leichtes, diese Datei wiederherzustellen.

Datenvernichtung unter Linux Systemen ist zwar ein wenig zuverlässiger, aber selbst in diesem Fall können wichtige Informationen mit speziellen Software-Tools wiederhergestellt werden.

Weder das Löschen von Partitionen noch das Formatieren der Datenträger löst das Problem dauerhaft. Wenn Partitionen einer

Festplatte gelöscht werden, geht die Information der Partitionstabelle oder die der Dateizuweisungstabelle (FAT) verloren. Allerdings bleibt die Information, die sich in den Sektoren befindet, völlig unberührt, so dass sie auch in diesem Fall fast mühelos wiederhergestellt werden kann.

Infolgedessen ist eine zuverlässige Datenvernichtung von Festplatten nur dann möglich, wenn eine speziell dafür entwickelte Software zum Einsatz kommt, die mit Löschalgorithmen arbeitet.

Garantierte Vernichtung sensibler Daten: Die Standards

Die Acronis DriveCleanser Software bietet eine garantierte Vernichtung sensibler Informationen mit Hilfe spezieller Methoden.

Acronis DriveCleanser Methoden garantieren eine Übereinstimmung mit den meisten bekannten nationalen Standards:

- USA: U.S. Standard, DoD 5220.22-M;
- USA: NAVSO P-5239-26 (RLL);
- USA: NAVSO P-5239-26 (MFM);
- Deutschland: VSITR;
- Russland: GOST P50739-95.

Neben Methoden, die den gerade erwähnten Standards entsprechen, unterstützt Acronis DriveCleanser vorgefertigte Methoden. Diese werden von namhaften Spezialisten auf dem Gebiet der Informationssicherheit vorgeschlagen.

- Peter Gutmann Algorithmus – Daten werden in 35 Durchläufen zerstört;
- Bruce Schneier Algorithmus – Daten werden in 7 Schritten vernichtet.

Acronis DriveCleanser unterstützt einfache und zugleich schnelle Löschmethoden, mit denen Sie die magnetischen Informationen in den Sektoren der Festplatten auf einen Nullwert bringen.

Doch das wichtigste Merkmal von Acronis DriveCleanser besteht aber in der Möglichkeit, einen eigenen Löschalgorithmus zur Datenvernichtung zu erstellen.

Für detaillierte Informationen über die verwendeten Methoden lesen Sie nach in Abschnitt in Kapitel 5, «Löschmethoden».

Nutzungsbedingungen der Software

Die Bedingungen für die Nutzung der Software Acronis DriveCleanser 6.0 sind in der Lizenzvereinbarung am Ende dieses Handbuchs beschrieben. Die einmalige Seriennummer ist der Nachweis für den legalen Erwerb und die Verwendung von Acronis DriveCleanser 6.0 auf Ihrem Computer. Sie ist auf der Box oder der CD-Fenstertasche angebracht, auf einer Lizenzurkunde enthalten oder wurde Ihnen in elektronischer Form übergeben. Es wird empfohlen, die Nummer durch Registrierung unter www.acronis.de/registration/ zu personalisieren, um über Produktupdates informiert zu werden und diese downloaden zu können.

Technische Unterstützung (Support)

Nutzer legal erworbener und registrierter Kopien von Acronis DriveCleanser 6.0 erhalten technische Unterstützung von Acronis. Im Problemfall sollten Sie jedoch zuerst versuchen, die Lösung in diesem Handbuch oder in der integrierten Programmhilfe zu finden.

Falls Sie Probleme mit der Installation oder Nutzung des Programms haben und diese weder mit dem Handbuch noch mit der Installationshilfe des Programms lösen können, besuchen Sie Zusammenstellung der häufig gestellten Fragen (FAQ) auf den Acronis-Internetseiten unter der Adresse http://www.acronis.de/support/.

Wenn Sie in der FAQ ebenfalls nicht fündig wurden, besuchen Sie die Seite http://www.acronis.de/my/support. Nach erfolgter Registrierung bzw. Anmeldung verwenden Sie das Kontaktformular für Ihre Anfrage. Dazu benötigen Sie die Seriennummer Ihrer Kopie von Acronis DriveCleanser 6.0, die Sie auf einer Lizenzurkunde finden oder die Ihnen in elektronischer Form übergeben wurde. Versuchen Sie, das Problem umfassend zu schildern und vergessen Sie nicht, die verwendete Hardware und die Version des Betriebssystems korrekt anzugeben.

Es wird vorausgesetzt, dass das Betriebssystem durch alle vorhandenen Servicepacks und Patches auf dem neuesten Stand ist, für die verwendete Hardware aktuelle Treiber installiert sind und Sie das neueste Build von Acronis DriveCleanser 6.0 benutzen.

Kapitel 2 Installation und erste Schritte

Bei einem Download des Programms erhalten Sie eine ausführbare Programmdatei und eine Seriennummer zur Freischaltung des Programms.

Die jeweils aktuellste Version des Handbuchs, die auch die eventuell in neuen Builds (Minor-Updates) hinzugekommenen oder veränderten Funktionen beschreibt, finden Sie im Internet unter http://www.acronis.de/enterprise/download/docs/. Zum Lesen ist eine Version von Adobe Acrobat Reader erforderlich.

Acronis DriveCleanser arbeitet mit einem Assistenten und nach einem einfachen Prinzip: Bei allen Aktionen stellen Sie zunächst mit Hilfe des Assistenten eine Handlungsanweisung (Skript) für Acronis DriveCleanser zusammen. Mit den üblichen Schaltflächen schreiten Sie z.B. schon während der Installation schrittweise **Weiter** voran, gehen bei Bedarf bereits gewählte Schritte zur Kontrolle bzw. Veränderung **Zurück** oder wählen **Abbrechen**, um den Vorgang nicht auszuführen.

Veränderungen an Datenträgern erfolgen in dieser Phase noch nicht. Durch Assistenten werden erst Veränderungen vorgenommen, wenn Sie auf **Fertig stellen** klicken. Bis zu diesem Befehl stellt Acronis DriveCleanser lediglich eine Handlungsfolge (Skript) zusammen, die Sie bis zur Bestätigung jederzeit ändern oder verwerfen können.

Diese einfache Bedienung der Assistenten wird im gesamten Handbuch vorausgesetzt: Es wird bei der Beschreibung der Abläufe meist nicht ausdrücklich darauf hingewiesen, dass Sie den jeweils nächsten Schritt eines Assistenten mit einem Klick auf die Schaltfläche **Weiter** auslösen müssen.

Systemanforderungen

Acronis DriveCleanser erfordert mindestens folgende Hardwareausstattung:

- Computer mit Prozessor der Pentium-Klasse oder höher
- 64 MB RAM
- FDD- oder CD-RW-Laufwerk für die Erstellung des bootfähigen Notfallmediums
- Maus (empfohlen).

Unterstützte Betriebssysteme

- Windows® 2000 Professional SP 4
- Windows® XP SP 2
- Windows XP Professional x64 Edition
- Windows® Vista (alle Editionen).

Installation von Acronis DriveCleanser

Führen Sie die Acronis DriveCleanser Installationsdatei aus und starten damit den Installationsvorgang. Folgen Sie aufmerksam der Installationsanleitung auf dem Bildschirm.

Nachdem Sie die Installation abgeschlossen haben, werden Sie aufgefordert eine bootfähige Diskette oder CD zu erstellen. Sollten Sie DriveCleanser unter Windows verwenden, so haben Sie mittels dieses Mediums die Möglichkeit, die Festplatten unter einem anderen Betriebssystem wie z.B. Linux zu löschen.

Wenn Sie nicht unter Windows arbeiten, dann sollten Sie in jedem Fall ein bootfähiges Medium erstellen, um von diesem Ihren Computer neu zu starten. Anschließend können Sie beliebige Partitionen löschen.

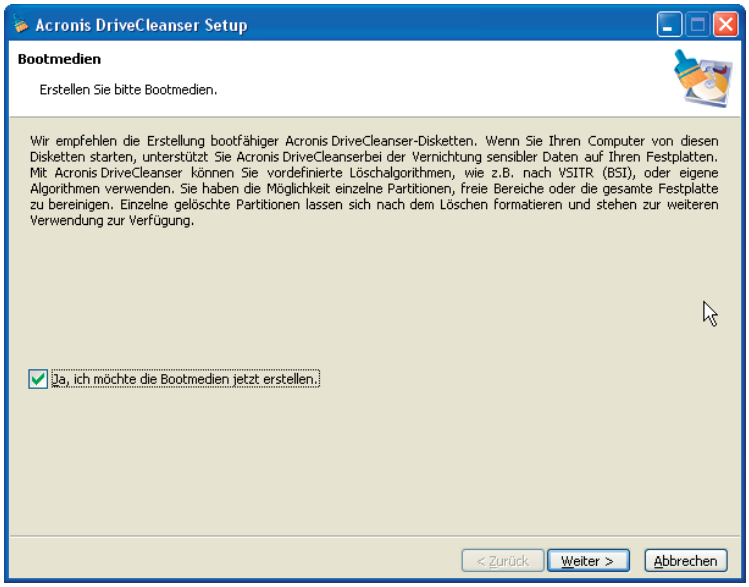

Abb. 1: Erstellen des Bootmediums

Nach Abschluss der Acronis DriveCleanser Installation werden Sie aufgefordert Ihren Rechner neu starten.

Reparatur / Upgrade Acronis DriveCleanser

Um Ihre Software zu reparieren oder auf den neuesten Stand zu bringen, starten Sie erneut die Installationsroutine. Das Installationsprogramm findet automatisch eine Version von DriveCleanser, die bereits auf Ihren Computer installiert wurde. Sie können entweder diese Version reparieren/upgraden oder deinstallieren.

Deinstallation der Software

Zum Deinstallieren der Software wählen Sie Acronis –> DriveCleanser –> Acronis DriveCleanser Deinstallieren in Ihrem Programmmenü. Es erscheint eine Dialogbox mit der Frage, ob sie diese Software wirklich entfernen möchten. Klicken Sie auf **JA,** um zu bestätigen. Im Anschluss daran wird Acronis DriveCleanser vollständig von Ihrem Computer entfernt.

Benutzeroberfläche

Acronis DriveCleanser benutzt eine windowsähnliche Oberfläche, die durch folgende Tasten **Tab, Shift+Tab, Links, Rechts, Oben , Unten**, **Leertaste**, **Enter** und **Escape** gesteuert werden kann.

Während Sie mit dem Acronis DriveCleanser arbeiten, werden Sie mit einer Reihe von Dialogfenstern konfrontiert. Sie müssen aus verschiedenen Optionen wählen und diverse Werte definieren, um schließlich eine gewünschte Partition bearbeiten zu können.

Die dazu jeweils notwendige Option wird entweder mit einem Mausklick oder einer Taste anwählbar.

Jedes Dialogfenster beinhaltet detaillierte und beschreibende Informationen über den Sinn und Zweck einer wählbaren Option. Außerdem finden Sie Kommentare für jedes Listenelement oder andere Einstellvarianten.

Kapitel 3 Löschen von Festplatten

Der Acronis DriveCleanser startet mit einem “Willkommen” Fenster. Dieses Fenster informiert Sie in erster Linie über die grundlegenden Möglichkeiten der Software. Diese sind wie folgt aufgeführt:

1. Löschen ausgewählter Festplatten mit einem vorgefertigten Lösch-Algorithmus.
2. Erstellen und Benutzen selbst erzeugter Methoden.

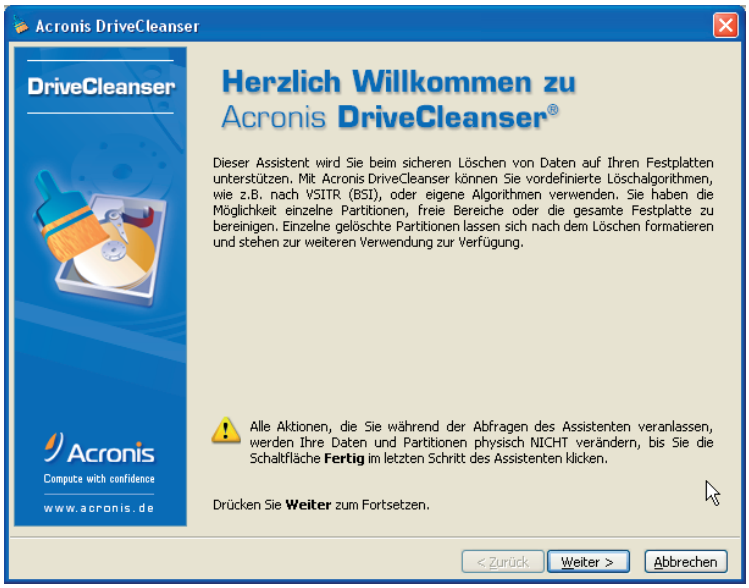

Abb. 2: Das erste Assistentenfenster

Alle Schritte späteren Schritte zur Datenzerstörung werden über ein Script gesteuert, das seine Informationen aus den Benutzereingaben bezieht. Es werden also nur dann Daten vernichtet, wenn Sie das Script ausführen.

Sie können jederzeit beliebig weit in den Einrichtungsschritten zurückgehen, um Einstellungen zu kontrollieren oder zu ändern. Zu diesen gehören z.B. die Auswahl einer Partition oder Änderung eines Löschalgorithmus.

Auswahl der Datenträger

Im zweiten Schritt des Assistenten – **Datenauswahl** – finden Sie die Konfiguration des Computers und die vorhandenen Partitionen

Computers. Im abgebildeten Beispiel wird eine Konfiguration zweier Festplatten angezeigt, die unter anderem Festplattenkapazität, Partitionsgrößen und Dateisystem enthält.

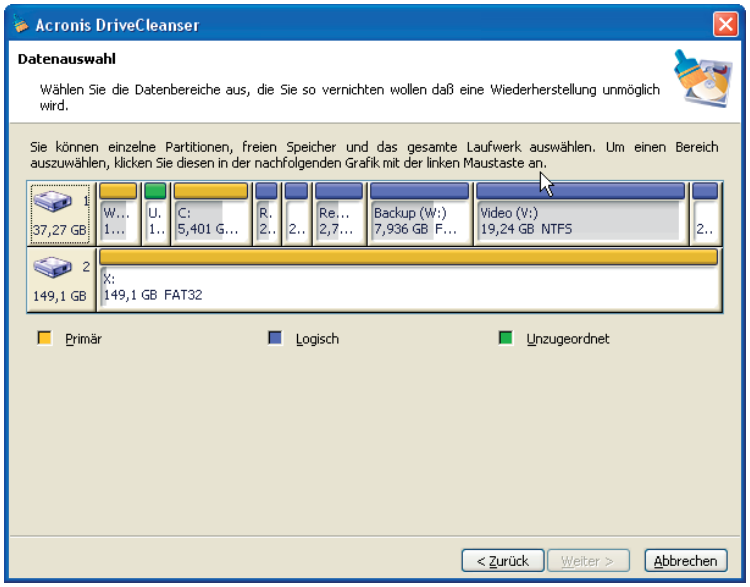

Abb. 3: Liste der Festplattenkonfiguration mit Partitionsangaben

Sie sind nun aufgefordert eine gewünschte Partition auszuwählen, die für eine Datenvernichtung gekennzeichnet werden soll.

Wenn Sie mit der Maus in ein Rechteck klicken, das für eine Partition steht, erscheint rechts oben ein kleines rotes Kreuz. Das bedeutet, dass die Partition für die Daten-Vernichtung ausgewählt wurde.

Selbstverständlich steht es Ihnen frei, eine oder mehrere Festplatten komplett zu markieren. Um diese Option zu nutzen, wählen Sie das Festplattensymbol links außen aus.

Sie können selbstverständlich mehrere Partitionen auf verschiedenen Festplatten gleichzeitig markieren.

Eine Einschränkung ist jedoch vorhanden: Wenn Sie Acronis DriveCleanser unter einem normalen Windowsbetriebssystem starten, dann kann die Systempartition natürlich nicht gelöscht werden. Für diesen Fall – z.B. beim totalen Beseitigen aller Festplatteninhalte auf einem alten Computer – erstellen Sie mit dem Builder für Bootmedien einen Datenträger, mit dem Sie den Rechner neu starten.

Im nachfolgenden Fenster – bietet Ihnen Acronis DriveCleanser drei Optionen zur Auswahl an:

- **Keine Änderung der Partition** – es werden mit Hilfe eines Algorithmus, den Sie später bestimmen, lediglich Daten vernichtet;
- **Löschen einer Partition** – es werden Daten vernichtet und die ausgewählte Partition entfernt;
- **Formatieren** – Daten werden vernichtet und die Partition formatiert (Standard).

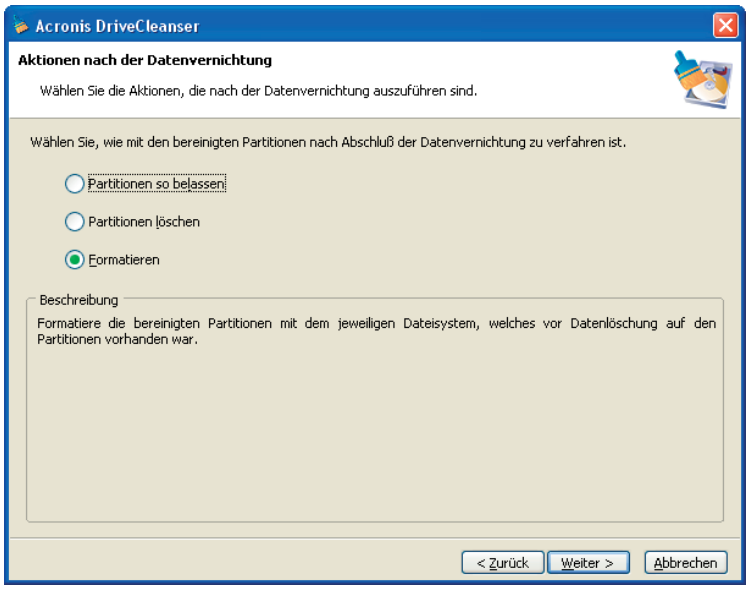

Abb. 4: Bestimmen Sie, was nach der Datenzerstörung passiert

Im nachfolgenden Beispiel wird davon ausgegangen, dass die erste Option (siehe oben) **Keine Änderung der Partition** ausgewählt wurde. Dieser Vorgang ermöglicht es Ihnen, ein objektives Bild von der **reinen** Datenvernichtung zu betrachten. Die Partition wird weder gelöscht noch entfernt.

Anwendung vordefinierter Löschmethoden

Nun müssen Sie einen Löschalgorithmus aus der unten aufgeführten Liste auswählen.

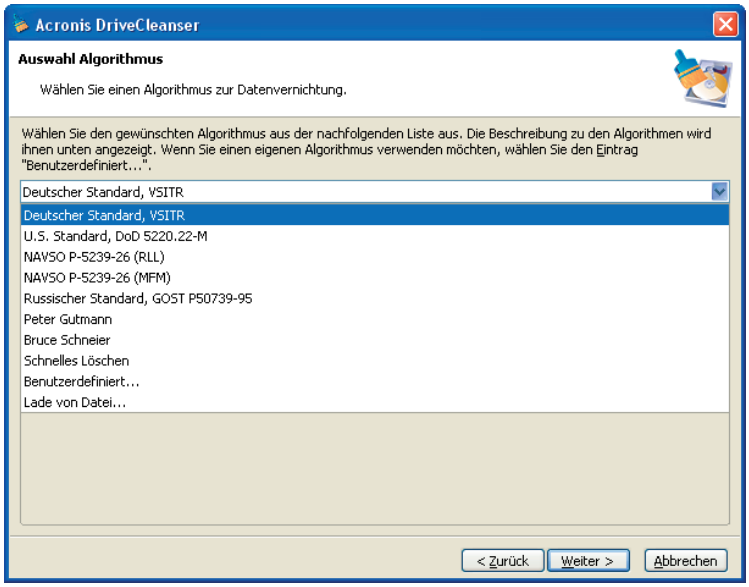

Abb. 5: Liste der definierten Löschmethoden

Das nächste Fenster stellt das Script für den ausgewählten Löschalgorithmus dar.

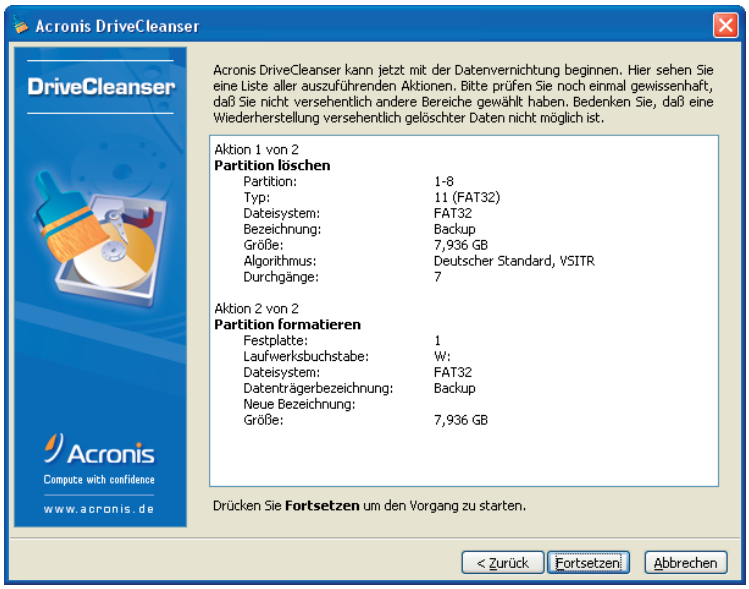

Abb. 6: Zusammenfasssung vor der Ausführung des Skripts

Der Acronis DriveCleanser kann nun mit der Datenvernichtung beginnen.

Klicken Sie den **Fortsetzen** Button an, um den Vorgang zu starten.

Nachdem Sie **Fortsetzen** angeklickt haben, kümmert sich der DriveCleanser automatisch um alles. Um den Vorgang endgültig abzuschließen, wird das Betriebssystem neu gestartet. Klicken auf **Fortsetzen**.

Nachdem der Vorgang abgeschlossen wurde, erhalten Sie eine Nachricht über die erfolgreich durchgeführte Datenvernichtung.

Kontrolle des Ergebnisses

Der Acronis DriveCleanser bietet anschließend eine Variante, um den “Löschbericht” Ihrer Festplatte bzw. Partition einzusehen. Die Software besitzt einen integrierten DiskViewer. Dieses Tool können Sie durch einen Klick auf die zugehörige Schaltfläche im Erfolgsfenster aktivieren.

Der bereits oben beschriebene Algorithmus bietet verschiedene Varianten der Datenvernichtung an. Deswegen hängt das Erscheinungsbild einer Partition bzw. Festplatte von der Auswahl eines Löschalgorithmus ab.

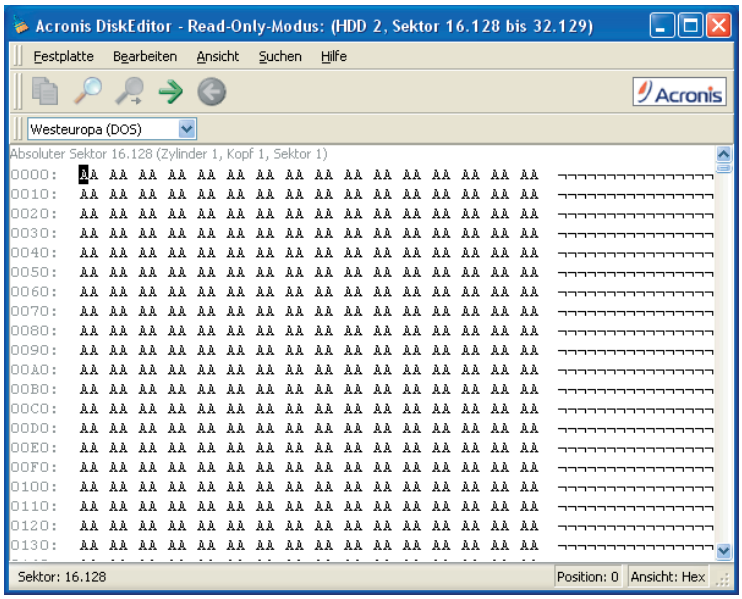

Abb. 7: Festplattensektor nach Ausführung eines „schnellen“ Algorithmus

Nach Einsicht in die Ergebnisse des Löschvorgangs schließen Sie den DiskEditor und beenden den Acronis DriveCleanser.

Kapitel 4 Erstellen eigener Löschmethoden

Acronis DriveCleanser bietet Ihnen die Möglichkeit, eigene Löschmethoden zur Datenvernichtung zu erstellen. Ungeachtet der Tatsache, dass die Software bereits Methoden aller Art enthält, steht es Ihnen natürlich frei, einen eigenen Löschalgorithmus zu kreieren.

Erstellen eigener Methoden

Das Fenster mit dem Script für die Datenvernichtung der jeweiligen Partition (eine Partition oder Festplatte wurde bereits zuvor ausgewählt) zeigt einen der vordefinierten Löschmethoden an. In diesem Fall wird der Wizard der Option **«Benutzerdefiniert...»** gestartet. Achten Sie an dieser Stelle auch auf die Option **«Lade von Datei...»**.

Um einen eigenen Algorithmus zu erstellen, wählen Sie in der **Algorithmus Auswahlliste** die Option **«Benutzerdefiniert...»** an.

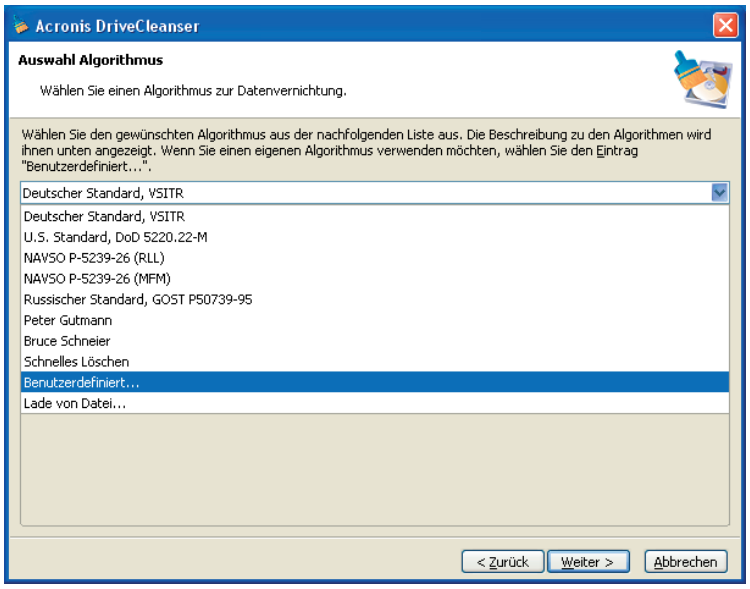

Abb. 8: Auswahl zur Erstellung eigener Methoden

Klicken Sie auf **Weiter**, um fort zufahren. Es erscheint ein Feld, das die Anzahl der Durchläufe definiert.

Als Beispiel soll ein Algorithmus dienen, der Ähnlichkeiten zum Amerikanischen Standard aufweist. Wie Sie vielleicht wissen, arbeitet der

Amerikanische Standard mit 3 Durchläufen, wobei verschiedene Symbole bzw. Zeichen (Samples) auf die Partition bzw. Festplatte geschrieben werden. Ein weiterer Durchlauf dient der Kontrolle. Insgesamt sind es also vier Durchläufe.

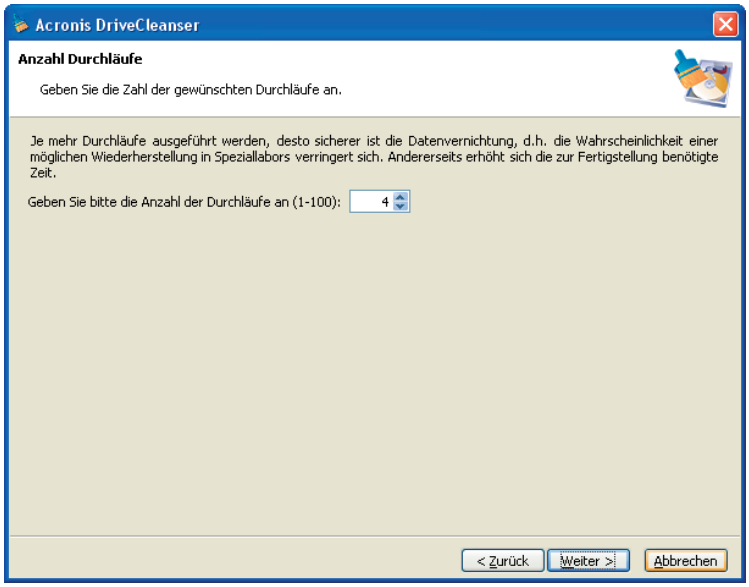

Abb. 9: Das Fenster mit der Anzahl von Durchläufen eines eigenen Algorithmus

Verschiedene Methoden führen unterschiedlich viele Durchläufe aus. Ein schneller Algorithmus, z.B. der russische Standard, führt z.B. nur einen aus, währenddessen der Algorithmus von Peter Gutmann bis zu 35 Schritte durchläuft.

Sie können jede beliebige Zahl von 1 bis 100 in das Feld per Maus oder Tastatur eintragen. Geben Sie z.B. die Ziffer 4 ein.

Klicken Sie auf **Weiter**, um fort zufahren.

Algorithmus-Definition: Vorlage

Der Schritt **Algorithmus-Definition** zeigt eine Vorlage des kommenden Algorithmus. Die Liste enthält eine Vielzahl Elemente, die den definierten Algorithmus aus dem vorherigen Schritt einschließt.

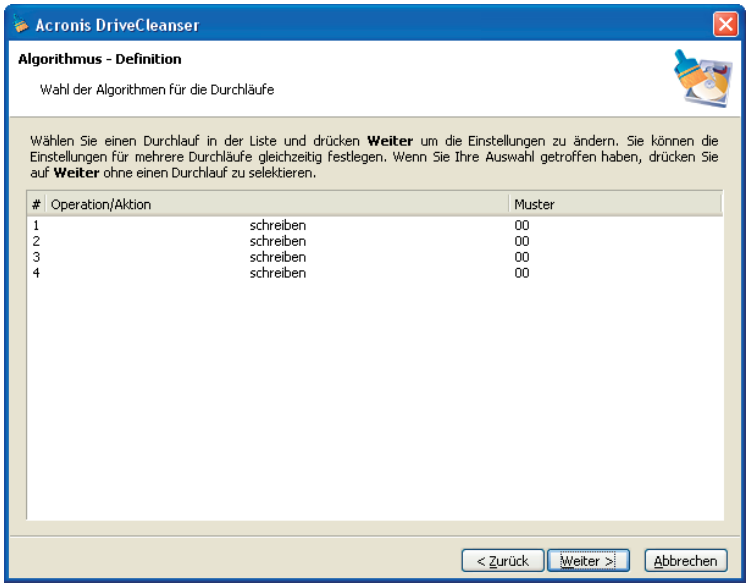

Abb. 10: Das Definitionsfenster für die Löschmethode

Die erste Spalte der Liste enthält die Anzahl von Durchläufen für eine Festplatte.

Die zweite Spalte stellt die Art der Operation dar. Dabei haben Sie die Wahl: Entweder wird ein Symbol auf die Festplatte geschrieben, oder die Festplatte bzw. Partition wird überprüft).

Die dritte Spalte zeigt das dem Muster, das auf die Partition geschrieben wird.

Beim gerade erwähnten Muster handelt es sich immer um einen hexadezimalen Wert wie z.B. 0x00, 0xAA, oder 0xCD. Diese Werte sind mindestens ein Byte groß und können bis 512 Bytes groß sein. Außer diesen Werten können Sie mit einem zufälligen Wert beliebiger Größe bis zu 512 Bytes arbeiten.

Eine weitere Alternative ist das Schreiben eines zum vorherigen Eintrag komplementären Wertes. Dabei wird die Information praktisch mit dem Gegenteil der vorherigen Information überschrieben.

Zur Erklärung: Z.B. wird ein binärer Wert von einer Sequenz 10001010 (0x8A) bei Auswahl der Komplementärmethode mit der Sequenz 01110101 (0x75) überschrieben.

So können Sie z.B. die folgenden Werte in Methoden einsetzen:

- Einen Hexadezimalwert 1 – 512 Bytes lang;
- Zufällige Hexadezimalwerte 1 – 512 Bytes lang;
- Hexadezimalwerte, die zu jenen komplementär sind, die im vorherigen Durchlauf auf die Festplatte geschrieben wurden.

Das Fenster **Algorithmus-Definition** liefert lediglich die Vorlage für den Algorithmus. Sie sollten daher sicher sein, was auf die Festplatte geschrieben wird, um vertrauliche Daten mittels des Algorithmus zu vernichten.

Veränderungen an einer der vorbereiteten Aktionen nehmen Sie vor, indem Sie die Aktion selektieren. Beginnen Sie mit den Festlegungen für den ersten Durchlauf.

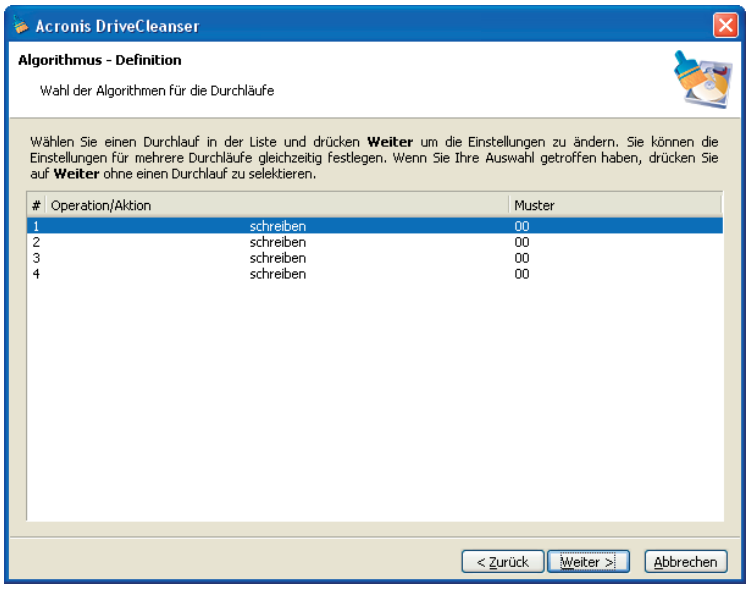

Abb. 11: Auswahl der Muster-Definition für den ersten Durchlauf

Klicken Sie auf **Weiter**, um fort zufahren.

Als nächstes sehen Sie ein Fenster, in dem Sie das zu schreibende Muster (hexadezimal) definieren.

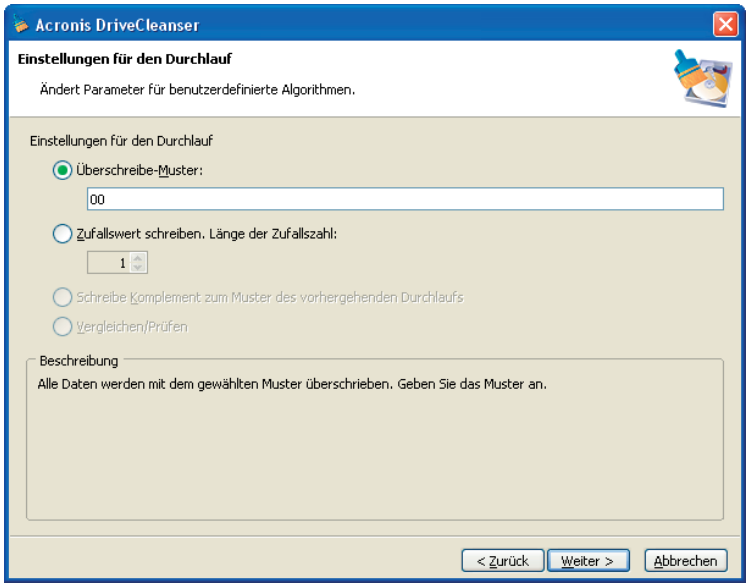

Abb. 12: Einstellungen für den Durchlauf

In der Abbildung ist die Option **Überschreibe-Muster** angewählt. Darunter befindet sich ein Feld, in welchem der hexadezimale Wert 0x00 eingetragen ist. Sie können jeden beliebigen hexadezimalen Wert in das Feld eintragen, damit er auf die Festplatte geschrieben wird.

Wenn Sie alternativ die Option **Zufallswert schreiben aktivieren**, dann definieren Sie anschließend die Größe des zufälligen Wertes im zugehörigen Einstellfeld.

Der amerikanische Standard sieht das Schreiben eines zufälligen Wertes in jedem Byte eines jeden Sektors im ersten Durchlauf an. Wählen Sie dazu z.B. **Zufallswert schreiben** aus und setzen Sie den Wert z.B. auf 1.

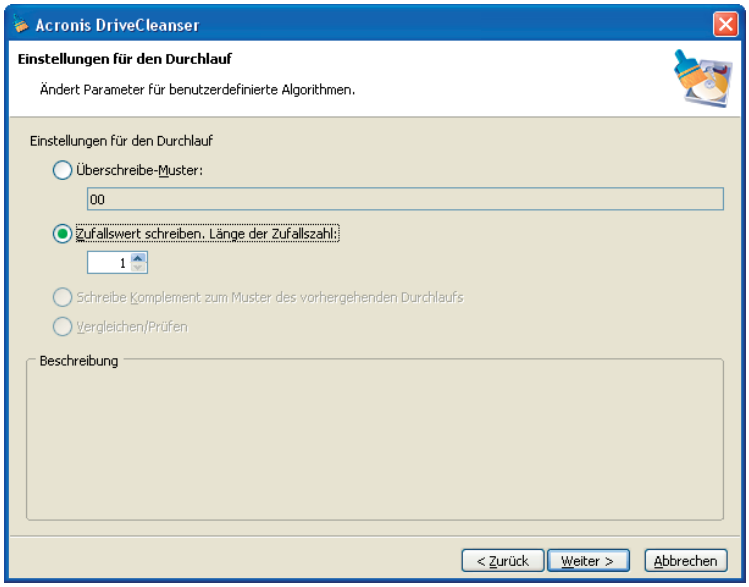

Abb. 13: Eingabe eines Zufallswerts mit der einem Byte Länge

Klicken Sie auf **Weiter**, um fort zufahren.

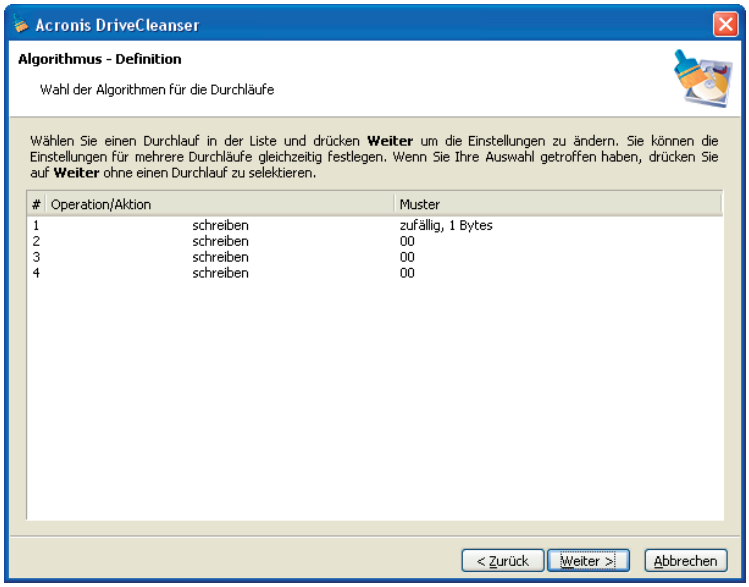

Abb. 14: Der erste Durchlauf des selbst erstellten Algorithmus ist definiert

Nach der Festlegung der Details für den Durchlauf gelangen Sie zurück in das Fenster mit allen Durchläufen. Die Anzeige hat sich auch verändert: Sie sehen nun die selbst festgelegten Vorgaben.

Um den zweiten nächste Durchlauf näher zu bestimmen, muss die zweite Zeile ausgewählt werden. Klicken Sie auf **Weiter**.

Nun sehen Sie erneut das Fenster mit den Details: Diesmal sind aber mehr Optionen als zuvor anwählbar. Hinzugekommen sind:

- **Schreibe Komplement zum Muster des vorhergehenden Durchlaufs**,
- **Vergleichen / Prüfen**.

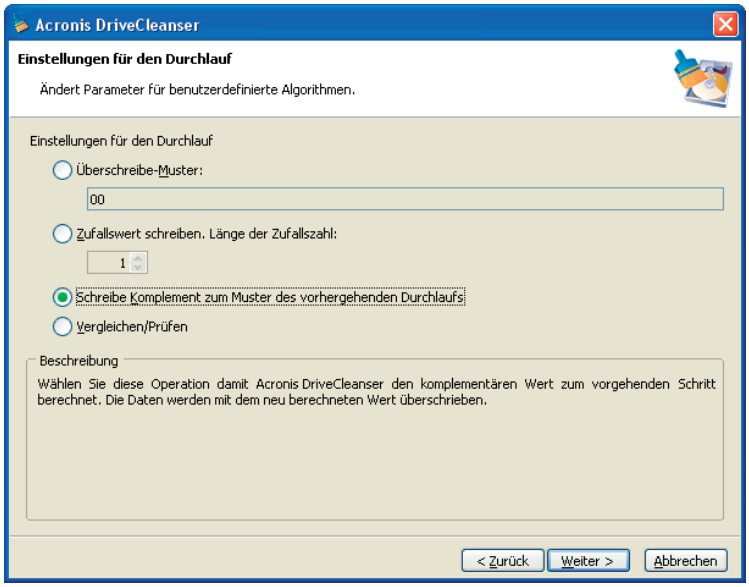

Abb. 15: Mit dieser Option wird der Komplementärwert berechnet.

Im Amerikanischen Standard wird im zweiten Durchlauf jeder Festplattensektor mit Hexadezimalwerten gefüllt, die zu jenen, die während des vorherigen Durchlaufs geschrieben wurden, komplementär sind. Im Beispiel wählen Sie die Option **Schreibe Komplement zum Muster des vorhergehenden Durchlaufs** und bestätigen mit **Weiter**.

Nach der Festlegung der Details für den zweiten Durchlauf gelangen Sie erneut zurück in das Fenster mit allen Durchläufen. Die Anzeige hat sich ebenfalls verändert: Sie sehen nun die selbst festgelegten Vorgaben für den zweiten Durchlauf.

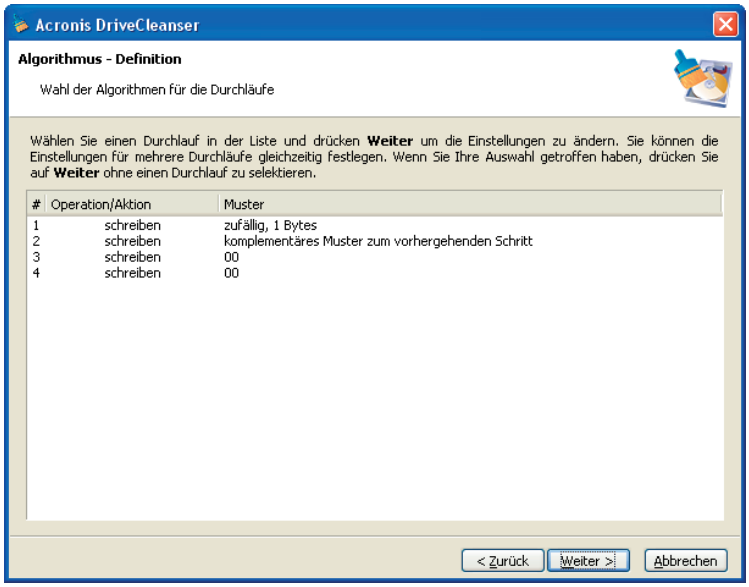

Abb. 16: Der zweite Durchlauf des selbst erstellten Algorithmus ist definiert

Auf die beschriebenen Art und Weise definieren Sie die weiteren Durchläufe. Je nach Ihren Vorstellungen oder Sicherheitsanforderungen erstellen Sie beliebige Datenvernichtungsmethoden.

Abschließend klicken Sie auf **Weiter**, ohne dass zuvor ein Durchgang definiert wurde. Damit gelangen Sie zu einem Fenster, in dem Sie den definierten Algorithmus für die Wiederverwendung speichern können.

Benutzerdefinierten Algorithmus speichern

Im nächsten Fenster **Benutzerdefinierten Algorithmus speichern** wählen Sie, ob Sie den eben definierten Algorithmus in einer Datei speichern oder ohne eine solche Speicherung fortfahren möchten.

Für die Speicherung wählen Sie die entsprechende Option und klicken auf **Weiter**. Um Ihren Algorithmus zu sichern, vergeben Sie einen Dateinamen und legen den jeweiligen Speicherort fest. Wählen Sie dazu das Datei Feld oder benutzen Sie den Explorer um eine bereits vorhandene Datei zu suchen und zu ersetzen. Der Name des Algorithmus sollte aussagefähig sein.

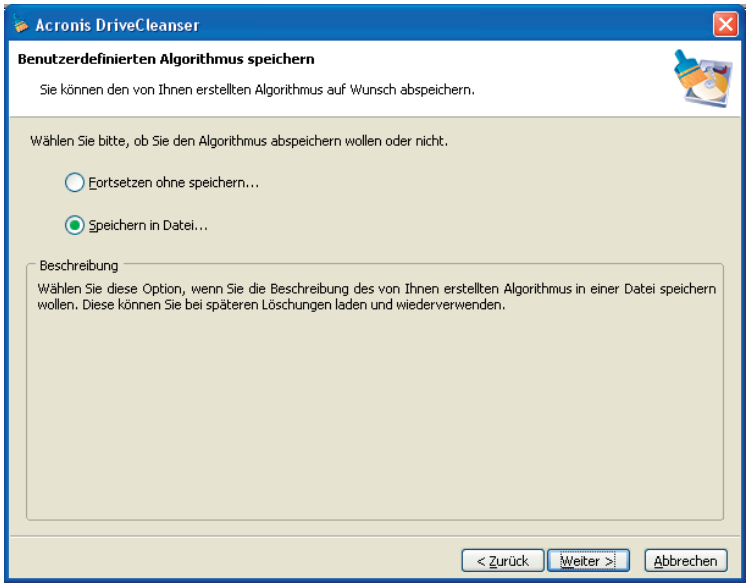

Abb. 17: Benutzerdefinierten Algorithmus speichern

Jeder selbst erstellte Algorithmus erhält einen spezifischen Namen und wird in einer eigenen Datei abgelegt. Sollten Sie versuchen einen neuen Algorithmus in einer existierenden Datei zu speichern, wird der bisherige Inhalt überschrieben.

Klicken Sie auf **Weiter**, um zum nächsten Fenster zu gelangen. Es zeigt das erstellte Lösch-Script, das auf Ihrem eigenen Algorithmus basiert.

Klicken Sie **Fortsetzen**, um das erstellte Script auszuführen.

Gespeicherten Algorithmus laden

Sollten Sie bereits einen Algorithmus mit dem Acronis DriveCleanser erstellt haben, können Sie den gespeicherten Algorithmus anstelle der im Programm vorgegebenen verwenden.

Wählen Sie in der **Auswahlliste** für den Algorithmus die Option **«Lade von Datei...»**.

In diesem Fall können Sie den Datenträger durchforsten, um die Datei mit dem gespeicherten Algorithmus zu finden. Alle anderen Schritte sind unverändert.

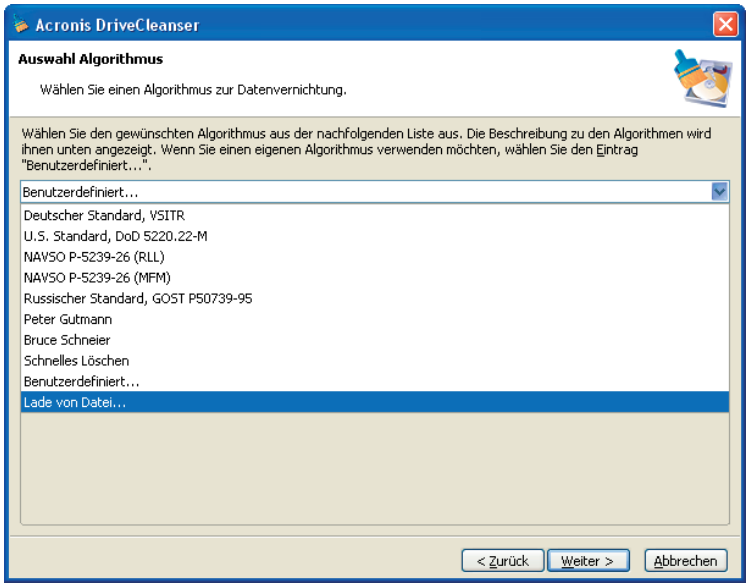

Abb. 18: Algorithmus Auswahlliste: Laden von Datei...

Kapitel 5 Löschmethoden

Informationen, die von Betriebssystem wie z.B. Windows gelöscht werden, können leicht wiederhergestellt werden. Mit Hilfe spezialisierter Software ist es möglich, selbst wiederholt mit anderen Daten überschriebene Informationen zu rekonstruieren. Dieses Problem kann nur durch spezielle Löschverfahren behoben werden.

Die **garantierte Datenvernichtung von Informationen** magnetische Medien, z.B. einer Festplatte, schließt eine Datenwiederherstellung durch qualifizierte Spezialisten mit entsprechender Software bzw. Methoden völlig aus.

Für die Begründung der gezielten Datenzerstörung ist ein kurzer Einblick in die Physik der Speichermedien erforderlich.

Die Daten werden auf einer Festplatte in binären Sequenzen mit 1 und 0 gesichert; die Sequenzen wiederum werden von unterschiedlich magnetisierten Teilen einer Festplatte repräsentiert. Dabei wird eine 1, die auf die Festplatte geschrieben wurde, vom Controller auch als solche 1 gelesen. Mit der 0 verhält es sich ebenso.

Wenn jedoch eine ursprünglich vorhanden 0 von einer 1 überschrieben wird, ist das Ergebnis nicht eine volle 1, sondern nur 0.95. Auch ist das Ergebnis beim Überschreiben einer 1 mit einer weiteren 1 nicht ebenfalls eins, sondern durch die Verstärkung des Magnetismus etwas größer, z.B. 1.05. Im praktischen Betrieb ist dieser Unterschied völlig irrelevant: Die Werte werden korrekt interpretiert. Mit einer speziellen Ausrüstung aber können die unter den aktuellen Daten liegenden Schichten herausgelesen werden, wenn die genauen Werte genommen werden. Dann rekonstruiert die spezialisierte Software zusammen mit einer leicht veränderten Hardware aus dem Wert 0.95 die vorher dort vorhandene Null. Dabei wird die Magnetisierung von Festplattensektoren und der restlichen Spuren analysiert und mit mikroskopischen Magnetverfahren wiederhergestellt.

Zusammenfassend für das Verständnis der nachfolgenden Methoden heißt das: Jeder Teil einer Festplatte speichert ein Abbild eines jeden Datensatzes, der je darauf geschrieben wurde. Der rekonstruierbare Effekt einer solchen „Datenaufzeichnung“ wird immer kleiner, je mehr Aufzeichnungen stattfinden.

Das Funktionsprinzip der Methoden

Das physikalische Löschen von Informationen erfordert die Änderung jedes magnetischen Bereichs auf der Festplatte. Der Vorgang muss so oft wie möglich mit speziell ausgewählten Schreibsequenzen in Folgen aus 1 und 0 (so genannten Sampels) wiederholt werden.

Bei der Benutzung der Verfahren zum logischen Verschlüsseln üblicher Festplatten können Sie über die Sampels entscheiden, die für das **wiederholte und wirksame Auslöschen jedweder Information** in den Schreibvorgängen benutzt werden**.**

Die von üblichen nationalen Standard-Methoden angebotenen zufälligen Zeichenfolgen für das Überschreiben der vorhandenen Daten (einfach oder dreifach) sind **willkürliche Festlegungen,** die lediglich in einfachen Fällen akzeptabel sind. Effektive Datenlöschungsmethoden basieren auf genauester Kenntnis der Feinheiten beim Schreiben von Daten auf jede Art von Festplatten. Diese Kenntnisse beweisen die Notwendigkeit komplexer mehrfacher Methoden, um die enthaltenen Informationen **garantiert** zu löschen.

Eine detaillierte Abhandlung über garantierte Datenvernichtung ist der folgende (englischsprachige) Artikel von Peter Gutmann.

http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html.

Von Acronis DriveCleanser genutzte Methoden

Die nachstehende Tabelle beschreibt kurz die Löschmethoden, die Acronis DriveCleanser benutzt. Jede Beschreibung enthält die Zahl der Schreibvorgänge und die Samples, mit denen jeder Sektor überschrieben wird.

Algorithmus (writing method)	Passes	Record
American: DoD 5220.22-M	4	1st pass – randomly selected symbols to each byte of each sector, 2 – complementary to written during the 1st pass; 3 – random symbols again; 4 – writing verification.

Algorithmus (writing method)	Passes	Record
American: NAVSO P-5239-26 (RLL)	4	1st pass – 0x01 to all sectors, 2 - 0x27FFFFF, 3 – random symbol sequences, 4 – verification.
American: NAVSO P-5239-26 (MFM)	4	1st pass – 0x01 to all sectors, 2 - 0x7FFFFFF, 3 – random symbol sequences, 4 – verification.
German: VSITR	7	1st – 6th – alternate sequences of: 0x00 and 0xFF; 7th - 0xAA; i.e. 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, 0xAA.
Russian: GOST P50739-95	1	Logical zeros (0x00 numbers) to each byte of each sector for 6th to 4th security level systems. Randomly selected symbols (numbers) to each byte of each sector for 3rd to 1st security level systems.
P. Gutmann's Algorithmus	35	Peter Gutmann's Algorithmus is very sophisticated. It's based on his theory of hard disk information wiping (see http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html).
B. Schneier's Algorithmus	7	Bruce Schneier offers seven pass overwriting Algorithmus in his Applied Cryptography book. 1st pass – 0xFF, 2st pass – 0x00, and then five times with a cryptographically secure pseudo-random sequence.
Schnell	1	Logical zeros (0x00 numbers) to all sectors to wipe.

ENDBENUTZER-LIZENZVERTRAG

Bitte lesen Sie die folgenden Bestimmungen sorgfältig durch.

Dieser Endbenutzer-Lizenzvertrag („EULA“) ist ein rechtsgültiger Vertrag zwischen Ihnen (entweder als natürliche oder juristische Person) und der Acronis Inc. (im Folgenden Acronis genannt). Er gilt sowohl für das in der Lizenzurkunde bezeichnete Produkt, als auch für alle sonstigen Acronis Produkte (das „SOFTWAREPRODUKT“) sowie alle Upgrades und Updates zum SOFTWAREPRODUKT. Er ist jeder vertriebenen Kopie des lizenzierten SOFTWAREPRODUKTS beizufügen.

Acronis DriveCleanser 6.0 (Das SOFTWAREPRODUKT) unterliegt dem Copyright © 2000-2007 der Acronis, Inc., in Deutschland vertreten durch die Acronis Germany GmbH, Balanstrasse 59, 81541 München. Alle Rechte sind vorbehalten. Durch die Nutzung des SOFTWAREPRODUKTS nehmen Sie diesen Lizenzvertrag an und erklären, dass Sie ihn gelesen und verstanden haben und mit allen seinen Bedingungen einverstanden sind. Acronis verzichtet ausdrücklich auf den Zugang der Annahmeerklärung (§ 151 BGB).

1. Lizenz

Acronis gewährt Ihnen als Käufer das nicht ausschließliche Recht, das erworbene SOFTWAREPRODUKT an so vielen Computer-Arbeitsplätzen bzw. Servern zu benutzen, wie in der Lizenzurkunde ausgewiesen. Eine Lizenz darf jeweils nur auf EINEM Computer eingesetzt werden. Das Recht ist nicht übertragbar, vermietbar oder verleihbar. Es ist nicht gestattet, das SOFTWAREPRODUKT anderen Nutzern, welche keine individuellen Lizenzen des SOFTWAREPRODUKTS besitzen, zur Nutzung im kommerziellen Computerservice, in Netzwerken, im Timesharing zur Verfügung zu stellen.

Das Kopieren und Archivieren des SOFTWAREPRODUKTS zum Zwecke der eigenen Datensicherung ist gestattet. Das Eigentum und die Urheberrechte oder sonstige Schutzrechte an dem SOFTWAREPRODUKT sowie an Dokumentationen, Handbüchern, Bedienungsanleitungen und sonstigen Materialien verbleiben nach wie vor bei Acronis.

2. Beschränkungen und Änderungsverbot

Das Programm oder Teile davon dürfen nicht kostenpflichtig oder kostenfrei weitergegeben, lizenziert, vermietet, verändert, übersetzt, angepasst oder veröffentlicht werden. Das SOFTWAREPRODUKT darf

weder im Gesamten noch in Teilen disassembliert, dekompiliert oder auf andere Weise in allgemein lesbare Form zurückgewandelt werden (Reverse Engineering).

3. Laufzeit des Vertrages

Die Lizenz gilt bis zu ihrer Beendigung. Der Lizenzvertrag kann dadurch beendet werden, dass das SOFTWAREPRODUKT sowie alle Kopien vernichtet werden. Die Lizenz erlischt unverzüglich, wenn gegen eine Bestimmung des Lizenzvertrages verstoßen wird, ohne dass es einer Kündigung durch Acronis, respektive seinen Vertriebspartnern, bedarf. Acronis bleibt zur Kündigung des Vertrages in diesem Fall gleichwohl berechtigt. Der ursprüngliche Käufer trägt gegenüber Acronis die Verantwortung für beliebige Schäden, die infolge einer Verletzung oder Nichtbeachtung des Lizenzvertrages entstehen.

4. Gewährleistungs-Ausschluss und Haftung

Acronis haftet bei Verbrauchern für die Dauer von 24 Monaten, bei Unternehmern für die Dauer von 6 Monaten, jeweils ab Übergabe des SOFTWAREPRODUKTS, das die CD-ROM/DVD, auf der das SOFTWAREPRODUKT gespeichert ist, frei von Mängeln ist, die die in der Dokumentation ausgewiesene Nutzung erheblich mindern. Acronis gewährleistet nicht, dass das SOFTWAREPRODUKT fehlerfrei betrieben werden kann oder dass beliebige Defekte beseitigt werden, das SOFTWAREPRODUKT oder dessen Funktionen Ihren Anforderungen sowie dem von Ihnen gewünschten Einsatzweck entsprechen.

Acronis übernimmt keine Gewähr für die Vollständigkeit und Richtigkeit des Inhaltes. Unternehmer müssen offensichtliche Mängel innerhalb einer Frist von einer Woche ab Empfang der Ware schriftlich anzeigen. Andernfalls ist die Geltendmachung eines Gewährleistungsanspruchs ausgeschlossen. Für andere, als durch Verletzung von Leben, Körper und Gesundheit entstehende Schäden haftet Acronis lediglich, soweit diese auf vorsätzlichem oder grob fahrlässigem Handeln oder auf schuldhafter Verletzung einer wesentlichen Vertragspflicht durch Acronis oder eines ihrer Erfüllungsgehilfen beruhen. Eine darüber hinausgehende Haftung für Schadensersatz ist ausgeschlossen. Soweit nicht grob fahrlässiges oder vorsätzliches Verhalten vorliegt, übernehmen Acronis oder ihre Vertriebspartner keine Haftung für:

1. beliebige Verluste die durch den Gebrauch des SOFTWAREPRODUKTS entstehen (einschließlich des Verlusts von Geschäftsgewinnen oder entgangenen Gewinnen in unbegrenzter Höhe),

2. Schäden an oder Verlust der gespeicherten Daten,

3. Geschäftsunterbrechung,

4. beliebige andere materielle oder immaterielle Verluste, die wegen der Benutzung oder der Verhinderung der Benutzung entstehen selbst dann nicht, wenn Acronis oder ihre Vertriebspartner über die Möglichkeit derartiger Verluste in Kenntnis gesetzt wurden. Etwaige Schadensersatzansprüche sind unabhängig von der Anspruchsgrundlage in der Höhe auf die entrichtete Lizenzgebühr beschränkt. Jegliche Ansprüche erlöschen in jedem Fall 24 Monate nach Lieferung.

5. Schlussbestimmungen

Es gilt deutsches Recht. Sollten einige Bestimmungen dieses Lizenzvertrages rechtlich unhaltbar oder unwirksam sein, bleiben alle anderen Bestimmungen rechtswirksam. Unwirksame Bestimmungen sind durch Regelungen zu ersetzen, die dem ursprünglichen Sinn am nächsten kommen.

