FreieSoftwareOG –

Papierkorb oder Schredder? - Dateien sicher löschen

Sicheres Löschen – Worum geht's hier eigentlich?

„Wie, sicheres löschen?“

„Wenn ich 

drücke, ist die Datei doch weg, oder?“

....

Sicheres Löschen – Worum geht's hier eigentlich?

- Dateien sind meistens nach dem einfachen Löschen mittels rm von der Festplatte mit speziellen Tools wiederherstellbar, da sie nicht physikalisch gelöscht, sondern nur mit einer Löschmarkierung versehen werden.
- Sie werden möglicherweise später überschrieben, wenn neue Dateien angelegt werden.

Sicheres Löschen – Worum geht's hier eigentlich?

- Bestimmt hat jeder von Zeit zu Zeit ein paar Dateien, die nicht für fremde Augen vorgesehen sind.
- Wenn man eine gebrauchte Festplatte verkaufen möchte, sollte man diese ebenfalls gründlich löschen, damit der eigene Lebenslauf, Bankdaten und Sonstiges nicht in falsche Hände geraten.

Sicheres Löschen – Worum geht's hier eigentlich?

- Sowohl das Dateisystem ext3/4 wie auch reiserfs erstellen immer ein Meta-Journal, welches Meta-Daten (unter anderem die Namen von Dateien) beinhalten kann.
- Diese von den Dateisystemen angelegten Journale können von Programmen nicht einfach überschrieben und gelöscht werden, wenn man nur Dateien überschreibt (beim Überschreiben einer ganzen Device-Datei besteht dieses Problem nicht).

Sicheres Löschen – Worum geht's hier eigentlich?

- Sie können Aufschluss über frühere auf der Festplatte vorhandene Dateien geben.
- Manche Dateisysteme und Journal-Modi speichern sogar ganze Dateien im Journal, welche dann auch aus dem Journal wieder rekonstruiert werden können, obwohl sie auf der Festplatte vollständig gelöscht und sogar mit wipe überschrieben wurden.

Sicheres Löschen – Worum geht's hier eigentlich?

- Noch schlechter sieht die Situation aus, wenn man keine „klassischen" (Magnet-)Festplatte verwendet, sondern einen Solid-State-Speicher, wie Flashlaufwerke oder USB-Sticks, deren Verhalten sehr fabrikat- und herstellerabhängig ist.
- Grundsätzlich ist es bei diesen Speichern nicht möglich, gezielt Blöcke auf dem Speicher zu überschreiben.
- Weder wipe noch shred funktionieren mit diesen Platten, wenn man nur einzelne Dateien sicher entfernen möchte.

Sicheres Löschen – Worum geht's hier eigentlich?

- Man sollte bei diesen vorsorgen und anstatt wichtige Dateien zu überschreiben, von Anfang an die entsprechenden Daten nur in verschlüsselter Form ablegen.
- Entweder indem man die Dateien einzeln mit GnuPG verschlüsselt, bevor man sie auf einen solchen Speicher ablegt oder indem man die einzelnen Partitionen auf dem Speicher an sich verschlüsselt.

Sicheres Löschen – Wozu eigentlich?

- Private Weitergabe bzw. Verkauf oder Entsorgung gebrauchter Hardware
- Schützen von Geschäftsdaten
- ...

Sicheres Löschen - Stolpersteine

- Flash-Speicher (USB-Sticks, SSDs)
- Defekte Sektoren
- Journaling

Sicheres Löschen – Stolperstein Flash-Speicher

- Verhalten ist stark Fabrikats- bzw. Herstellerabhängig
- Grundsätzlich ist es nicht möglich, gezielt Blöcke auf dem Speicher zu überschreiben
- Schreibzyklen sind (je nach Bauart) begrenzt
- Deshalb wird Wear-Leveling vom integrierten Controller
- Verwendet (Daten werden gleichmäßig verteilt)
- Moderne Flash-Speicher verwenden eine interne Garbage Collection des Controllers oder den TRIM-Befehl des Betriebssystems

Sicheres Löschen - Stolpersteine

Deshalb:

Verschlüsseln (Einzelne Dateien oder ganze Partition)

Sicheres Löschen – Stolperstein defekte Sektoren

Defekte Sektoren werden solange nicht bemerkt, wie noch Erstzsektoren bereit stehen.

- Controller verwaltet diese gegenüber dem Betriebssystem transparent
- Daten in defekten Sektoren bleiben erhalten
- Kontrolle vorhandener defekter Sektoren ist möglich
  - mit smartmontools ("*smartctl -a /dev/sda grep Reallocated_Sector_Ct*")

Sicheres Löschen – Stolperstein Journaling

- Ext3/4, reiserfs und btrfs erstellen immer ein Meta-Journal, welches Meta-Daten (unter anderem die Namen von Dateien) beinhalten kann.
- Manche Dateisysteme und Journal-Modi speichern sogar ganze Dateien im Journal, welche dann auch aus dem Journal wieder rekonstruiert werden können, obwohl sie auf der Festplatte vollständig gelöscht und sogar mit wipe überschrieben wurden...

Sicheres Löschen - Stolpersteine

- Das Löschen einzelner Dateien oder Verzeichnisse hat keinen Einfluss auf den MBR
- Hier setzen sich auch Schadprogramme fest
- Löschen von Partitionen bzw. Formatieren der Festplatte nützen nichts

Sicheres Löschen - Löschmethoden

- Gutmann-Methode (1996)
- Russian GOST P50739-95
- Bruce Schneier's Algorithmus

Ist es wirklich notwendig, einen Datenträger 35-fach zu überschrieben, um sicher zu sein, dass nichts mehr rekonstruierbar ist?

Craig Wright behauptet: NEIN! (Studie von 2009).

Bereits das einmalige Überschreiben lässt keine Chance für Forensiker

Sicheres Löschen – Die Werkzeuge für Dateien

- shred

  überschreibt Dateien oder Device-Dateien (z.B. Partitionen) und löscht sie danach, wenn gewünscht. Shred arbeitet dabei nach der Gutmann-Methode. Im Gegensatz zu wipe kann shred keine Ordner löschen.

- wipe

  ist ein Kommandozeilenprogramm zum sicheren Löschen und Überschreiben von Dateien, Ordnern und Device-Dateien (z.B. Partitionen). Wipe kann auch Ordner löschen und bietet mehr Einstellungsmöglichkeiten

Sicheres Löschen – Die Werkzeuge für Datenträger

- dd (*dd if=/dev/zero of=/dev/sda*)
- wipe (*wipe -k /dev/sda7*)
- shred (*shred -vn 2 /dev/sda*)
- Plattenputzer (unmaintained)
- DBAN (Freie Version unmaintained)

LPI - Fragen

LPI - Frage #15

Wie heißt die Konfigurationsdatei, welche vom syslog-Daemon verwendet wird?

A) syslog.conf
B) syslogd
C) slog.conf
D) system.conf

Antwort: A
Beispiel: cat /etc/syslog.conf (rsyslog.conf)

Bitte beachten

Auf der Homepage findet sich immer das

aktuelle Datum, sowie das Thema des nächsten Treffens!

Weitergehende Informationen

https://wiki.ubuntuusers.de/Daten_sicher_l%C3%B6schen/

xxx

xxx

xxx

Weitere Informationen bekommen Sie hier:

http://www.FreieSoftwareOG.org

und

Kontakt@FreieSoftwareOG.org

oder kommen Sie doch einfach zu unserem regelmäßigen Treffen,
jeden 1. Mittwoch im Monat ab 20:00 Uhr.
(Treffpunkt laut Webseite)