Linux-Info-Tag 2013

Datenträger einfach verschlüsseln für Einsteiger

Mike Koreny

6. Februar 2013

Inhaltsverzeichnis

Inhaltsverzeichnis

Inhaltsverzeichnis

Inhaltsverzeichnis

Inhaltsverzeichnis

Inhaltsverzeichnis

Warum sollte ich meine Daten verschlüsseln?

Warum sollte ich meine Daten verschlüsseln?

- Das Laufwerk oder Notebook wird gestohlen oder irgenwo liegen gelassen.

Warum sollte ich meine Daten verschlüsseln?

Warum sollte ich meine Daten verschlüsseln?

- Das Laufwerk oder Notebook wird gestohlen oder irgenwo liegen gelassen.
- Das Laufwerk oder Notebook wird zur Reparatur eingeschickt.

Warum sollte ich meine Daten verschlüsseln?

Warum sollte ich meine Daten verschlüsseln?

- Das Laufwerk oder Notebook wird gestohlen oder irgenwo liegen gelassen.
- Das Laufwerk oder Notebook wird zur Reparatur eingeschickt.
- Das Laufwerk, beispielweise ein externer Datenträger, wird verkauft.

Und was habe ich zu verbergen?

Hypothese

Wir sind alle nur Menschen. **Jeder** hat irgendein dunkles Geheimnis auf seiner Festplatte!

Und was habe ich zu verbergen?

Hypothese

Wir sind alle nur Menschen. **Jeder** hat irgendein dunkles Geheimnis auf seiner Festplatte!

Beispiele

Und was habe ich zu verbergen?

Hypothese

Wir sind alle nur Menschen. **Jeder** hat irgendein dunkles Geheimnis auf seiner Festplatte!

Beispiele

- private Korrespondenz, beispielsweise mit dem Rechtsanwalt oder Steuerberater

Und was habe ich zu verbergen?

Hypothese

Wir sind alle nur Menschen. **Jeder** hat irgendein dunkles Geheimnis auf seiner Festplatte!

Beispiele

- private Korrespondenz, beispielsweise mit dem Rechtsanwalt oder Steuerberater
- ausgesprochen private Briefe (Freund im Knast, Liebesbriefe)

Und was habe ich zu verbergen?

Hypothese

Wir sind alle nur Menschen. **Jeder** hat irgendein dunkles Geheimnis auf seiner Festplatte!

Beispiele

- private Korrespondenz, beispielsweise mit dem Rechtsanwalt oder Steuerberater
- ausgesprochen private Briefe (Freund im Knast, Liebesbriefe)
- oben ohne Strandfotos (der Freundin) aus dem letzten Urlaub

Und was habe ich zu verbergen?

Hypothese

Wir sind alle nur Menschen. **Jeder** hat irgendein dunkles Geheimnis auf seiner Festplatte!

Beispiele

- private Korrespondenz, beispielsweise mit dem Rechtsanwalt oder Steuerberater
- ausgesprochen private Briefe (Freund im Knast, Liebesbriefe)
- oben ohne Strandfotos (der Freundin) aus dem letzten Urlaub
- gerippte Musikdateien (Sicherungskopien), für die man evtl. nicht mehr die Original-CD besitzt

Und was habe ich zu verbergen?

Hypothese

Wir sind alle nur Menschen. **Jeder** hat irgendein dunkles Geheimnis auf seiner Festplatte!

Beispiele

- private Korrespondenz, beispielsweise mit dem Rechtsanwalt oder Steuerberater
- ausgesprochen private Briefe (Freund im Knast, Liebesbriefe)
- oben ohne Strandfotos (der Freundin) aus dem letzten Urlaub
- gerippte Musikdateien (Sicherungskopien), für die man evtl. nicht mehr die Original-CD besitzt

Aufgepasst!

Nun gehe die obigen Punkte noch einmal aufmerksam durch, und denke dabei besonders an bereits gelöschte Dateien!

Das Experiment: forensische Datenanalyse

Bitte machen Sie das nicht zu Hause nach!

Für dieses Praxisbeispiel nehmen wir uns einen Datenträger mit Daten.
Wir werden

Das Experiment: forensische Datenanalyse

Bitte machen Sie das nicht zu Hause nach!

Für dieses Praxisbeispiel nehmen wir uns einen Datenträger mit Daten. Wir werden

- alle darauf enthaltenen Dateien löschen,

Das Experiment: forensische Datenanalyse

Bitte machen Sie das nicht zu Hause nach!

Für dieses Praxisbeispiel nehmen wir uns einen Datenträger mit Daten. Wir werden

- alle darauf enthaltenen Dateien löschen,
- den Datenträger anschließend partitionieren

Das Experiment: forensische Datenanalyse

Bitte machen Sie das nicht zu Hause nach!

Für dieses Praxisbeispiel nehmen wir uns einen Datenträger mit Daten. Wir werden

- alle darauf enthaltenen Dateien löschen,
- den Datenträger anschließend partitionieren
- und formatieren.

Das Experiment: forensische Datenanalyse

Bitte machen Sie das nicht zu Hause nach!

Für dieses Praxisbeispiel nehmen wir uns einen Datenträger mit Daten. Wir werden

- alle darauf enthaltenen Dateien löschen,
- den Datenträger anschließend partitionieren
- und formatieren.

`foremost`

Der Originalcode von foremost wurde von Special Agent Kris Kendall und Special Agent Jesse Kornblum vom United States Air Force Office of Special Investigations geschrieben. (Quelle: manpage)
foremost erkennt viele Dateitypen anhand ihrer Datei-Header, Datei-Footer und den Datenstrukturen und stellt erkannte Dateien wieder her.

Und so wird's gemacht! - Wir löschen die Daten ...

alle vorhandenen Daten löschen

```
$ sudo rm -r /media/F33E-0541/*
```

Und so wird's gemacht! - Wir löschen die Daten ...

alle vorhandenen Daten löschen

```
$ sudo rm -r /media/F33E-0541/*
```

Datenträger neu partitionieren

```
$ sudo umount /media/F33E-0541
$ sudo fdisk /dev/sdb
```

Und so wird's gemacht! - Wir löschen die Daten ...

alle vorhandenen Daten löschen

```
$ sudo rm -r /media/F33E-0541/*
```

Datenträger neu partitionieren

```
$ sudo umount /media/F33E-0541
$ sudo fdisk /dev/sdb
```

Datenträger formatieren

```
$ sudo mkfs.ext3 /dev/sdb1
```

Und so wird's gemacht! - Und stellen sie wieder her ...

foremost installieren

```
$ sudo apt-get install foremost
```

Und so wird's gemacht! - Und stellen sie wieder her ...

`foremost` installieren

```
$ sudo apt-get install foremost
```

Datenträger-Image auslesen

```
$ sudo dd if=/dev/sdb of=image.dd
```

Und so wird's gemacht! - Und stellen sie wieder her ...

foremost installieren

```
$ sudo apt-get install foremost
```

Datenträger-Image auslesen

```
$ sudo dd if=/dev/sdb of=image.dd
```

foremost mit Standard-Optionen ausführen

```
$ foremost image.dd
```

Was könnten wir gegen diese Art der Datenanalyse tun?

Den Datenträger komplett mit Nullen oder Zufallsdaten überschreiben

```
$ sudo shred /dev/sdb
```

`shred` überschreibt den Datenträger oder die Datei mehrfach mit Zufallsdaten. Eine Wiederherstellung ist dann eigentlich unmöglich!

Was könnten wir gegen diese Art der Datenanalyse tun?

Den Datenträger komplett mit Nullen oder Zufallsdaten überschreiben

```
$ sudo shred /dev/sdb
```

`shred` überschreibt den Datenträger oder die Datei mehrfach mit Zufallsdaten. Eine Wiederherstellung ist dann eigentlich unmöglich!

- Das kann bei einem größeren Datenträger sehr zeitaufwendig sein!

Was könnten wir gegen diese Art der Datenanalyse tun?

Den Datenträger komplett mit Nullen oder Zufallsdaten überschreiben

```
$ sudo shred /dev/sdb
```

`shred` überschreibt den Datenträger oder die Datei mehrfach mit Zufallsdaten. Eine Wiederherstellung ist dann eigentlich unmöglich!

- Das kann bei einem größeren Datenträger sehr zeitaufwendig sein!
- Bietet keinen Schutz bei Diebstahl!

Was könnten wir gegen diese Art der Datenanalyse tun?

Den Datenträger komplett mit Nullen oder Zufallsdaten überschreiben

```
$ sudo shred /dev/sdb
```

`shred` überschreibt den Datenträger oder die Datei mehrfach mit Zufallsdaten. Eine Wiederherstellung ist dann eigentlich unmöglich!

- Das kann bei einem größeren Datenträger sehr zeitaufwendig sein!
- Bietet keinen Schutz bei Diebstahl!
- Keine vernünftige Lösung, wenn der Datenträger oder das Notebook nur vorübergehend, beispielsweise zur Reparatur, aus der Hand gegeben wird.

Der Verschlüsselungsalgorythmus

Ausgabe von `cryptsetup --help`:

```
Vorgabewerte für Schlüsseldatei:
Maximale Größe der Schlüsseldatei:  8192kB, Maximale Länge
des interaktiven Passsatzes:  512 Zeichen
Standard-Verschlüsselungsparameter:
Loop-AES: aes, Schlüssel 256 Bits
plain:  aes-cbc-essiv:sha256, Schlüssel:  256 Bits,
Passsatz-Hashen:  ripemd160
LUKS1:  aes-cbc-essiv:sha256, Schlüssel:  256 Bits,
LUKS-Kopfbereich-Hashen:  sha1, Zufallszahlengenerator:
/dev/urandom
```

Sichere Passworte

Was versteht man unter einem sicheren Passwort?

Ein **s**icheres **P**asswort **e**nthält **m**indestens **8** **Z**eichen**, d**arunter **g**roße **u**nd **k**leine **B**uchstaben**, $**onderzeichen **u**nd **Z**ahlen**.**

Sichere Passworte

Was versteht man unter einem sicheren Passwort?

Ein **s**icheres **P**asswort **e**nthält **m**indestens **8 Z**eichen**, d**arunter **g**roße **u**nd **k**leine **B**uchstaben**, $**onderzeichen **u**nd **Z**ahlen**.**

Und so sieht es aus:

EsPem8Z,dgukB,$uZ.

dm-crypt / LUKS

dm-crypt

dm-crypt / LUKS

dm-crypt

- dm-crypt ist ein Verschlüsselungsmodul des Device-Mappers im Linux-Kernel

dm-crypt / LUKS

dm-crypt

- dm-crypt ist ein Verschlüsselungsmodul des Device-Mappers im Linux-Kernel
- dm-crypt verschlüsselt beliebige Gerätedateien aus Sicht des Benutzers transparent

dm-crypt / LUKS

dm-crypt

- dm-crypt ist ein Verschlüsselungsmodul des Device-Mappers im Linux-Kernel
- dm-crypt verschlüsselt beliebige Gerätedateien aus Sicht des Benutzers transparent

LUKS (Linux Unified Key Setup)

dm-crypt / LUKS

dm-crypt

- dm-crypt ist ein Verschlüsselungsmodul des Device-Mappers im Linux-Kernel
- dm-crypt verschlüsselt beliebige Gerätedateien aus Sicht des Benutzers transparent

LUKS (Linux Unified Key Setup)

- LUKS ist eine gängige Erweiterung zu dm-crypt

dm-crypt / LUKS

dm-crypt

- dm-crypt ist ein Verschlüsselungsmodul des Device-Mappers im Linux-Kernel
- dm-crypt verschlüsselt beliebige Gerätedateien aus Sicht des Benutzers transparent

LUKS (Linux Unified Key Setup)

- LUKS ist eine gängige Erweiterung zu dm-crypt
- LUKS erweitert das verschlüsselte Gerät um einen Header in dem Metadaten sowie bis zu acht Schlüssel gespeichert werden

dm-crypt / LUKS

dm-crypt

- dm-crypt ist ein Verschlüsselungsmodul des Device-Mappers im Linux-Kernel
- dm-crypt verschlüsselt beliebige Gerätedateien aus Sicht des Benutzers transparent

LUKS (Linux Unified Key Setup)

- LUKS ist eine gängige Erweiterung zu dm-crypt
- LUKS erweitert das verschlüsselte Gerät um einen Header in dem Metadaten sowie bis zu acht Schlüssel gespeichert werden
- Der Datenträger wird als verschlüsseltes Gerät erkannt

dm-crypt / LUKS

dm-crypt

- dm-crypt ist ein Verschlüsselungsmodul des Device-Mappers im Linux-Kernel
- dm-crypt verschlüsselt beliebige Gerätedateien aus Sicht des Benutzers transparent

LUKS (Linux Unified Key Setup)

- LUKS ist eine gängige Erweiterung zu dm-crypt
- LUKS erweitert das verschlüsselte Gerät um einen Header in dem Metadaten sowie bis zu acht Schlüssel gespeichert werden
- Der Datenträger wird als verschlüsseltes Gerät erkannt
- Die Schlüssel können einzeln deaktiviert oder geändert werden, ohne das ganze Dateisystem neu verschlüsseln zu müssen

Vorbereitung

cryptsetup

Das Programm `cryptsetup` sollte installiert sein

```
$ sudo apt-get install cryptsetup
```

Vorbereitung

cryptsetup

Das Programm `cryptsetup` sollte installiert sein

```
$ sudo apt-get install cryptsetup
```

dm-crypt

Das Kernelmodul `dm-crypt` sollte geladen sein

```
$ sudo modeprobe dm-crypt
```

Vorbereitung

cryptsetup

Das Programm `cryptsetup` sollte installiert sein

```
$ sudo apt-get install cryptsetup
```

dm-crypt

Das Kernelmodul `dm-crypt` sollte geladen sein

```
$ sudo modeprobe dm-crypt
```

Datenträger

Es wird ein Datenträger benötigt - Achtung, alle bisher gespeicherten Daten werden gelöscht!

Auf geht's ...

Datenträger mit Zufallsdaten überschreiben

```
$ sudo dd if=/dev/urandom of=/dev/sdb
```

Hintergrund: so können auch keine früher gespeicherten unverschlüssleten Daten ausgelesen werden und zusätzlich werden Angriffe auf die Verschlüsselung erschwert

Auf geht's ...

Datenträger mit Zufallsdaten überschreiben

```
$ sudo dd if=/dev/urandom of=/dev/sdb
```

Hintergrund: so können auch keine früher gespeicherten unverschlüssleten Daten ausgelesen werden und zusätzlich werden Angriffe auf die Verschlüsselung erschwert

Datenträger neu partitionieren

```
$ sudo fdisk /dev/sdb
```

Auf geht's ...

Datenträger mit Zufallsdaten überschreiben

```
$ sudo dd if=/dev/urandom of=/dev/sdb
```

Hintergrund: so können auch keine früher gespeicherten unverschlüssleten Daten ausgelesen werden und zusätzlich werden Angriffe auf die Verschlüsselung erschwert

Datenträger neu partitionieren

```
$ sudo fdisk /dev/sdb
```

Datenträger für Verschlüssellung einrichten und formatieren

```
$ sudo luksformat -t ext3 /dev/sdb1
```

Weiterführende Informationen

foremost

Manpage: (`$ man foremost`)

dm-crypt und LUKS

Internet: `de.wikipedia.org/wiki/Dm-crypt`

AES (Advanced Encryption Standard)

Internet: `de.wikipedia.org/wiki/Advanced_Encryption_Standard`

Weitere Hilfestellung zur Verschlüsselung mit dm-crypt und LUKS

Internet: `wiki.laub-home.de/wiki/Festplatten_Verschl%C3%BCsselung_mit_luks_und_dmcrypt`

Fragen?

? ? ?