Sichere Daten - verschlüsseln von Festplatten

Sebastian Andres sebastian@sebastianandres.de
13. März 2010 Linuxtage Chemnitz

Übersicht

- Grundlagen
- Wichtige Hinweise!
- Praxis: verschlüsseln eines USB-Sticks
- Befehlsübersicht Cryptsetup

Grundlagen

- Unterschied zu gpg (GPG verschlüsselt dateien). Cryptsetup setzt eine ebene tiefer an, das komplette Dateisystem wird verschlüsselt.
- Warum cryptsetup? (Ist im Kernel integriert, Kann in initrd integriert werden, kann mehrere passwörter verwenden, etc.)
- Wo setzt cryptsetup an? (Unterhalb des Dateisystems) – daher ist das komplette System verschlüsselt.
- Bereits bei der Installation kann verschlüsselung gewählt werden. Das Root-Filesystem (/) kann nachträglich schlecht bzw. nur mit sehr hohem Aufwand verschlüsselt werden.

Wichtige Hinweise

- Kein schutz von Außen! ist die Partition offen, kann jeder möglicherweise aus dem Internet zugriff bekommen! Geschützt sind die Daten nur vor Personen, welche den Rechner (Hardwaremäßig) physikalisch öffnen und die Festplatten Ausbauen wollen, oder mit einer Live-CD das System booten.
- Sicher sind die Daten nur, wenn die Partition verschlossen, bzw. der Rechner abgeschaltet ist.
- Was ist mit Swap? Zu bedenken gilt, das sowohl der Ram als auch die Swap-Partition unter umständen nicht verschlüsselt ist (Die Swap-Partition kann selbstverständlich verschlüsselt werden!).

Praxis

- Praktisches Beispiel: USB-Stick verschlüsseln

Befehlsübersicht

Befehl	Beschreibung
cryptsetup -c aes-cbc-essiv:sha256 -y -s 256 luksFormat /dev/hda7	Legt eine verschlüsselte Partition (In diesem Fall hda7) neu an. VORSICHT!!! Alle daten auf dieser Partition gehen dabei verloren!
cryptsetup luksOpen /dev/hda7 crypt_name	Öffnet die Partition hda7. crypt_name kann dabei frei gewählt werden – das geöffnete device ist unter /dev/mapper zu finden.
cryptsetup luksClose crypt_name	Schließt die Partition (hda7) wieder ab.
cryptsetup luksAddKey /dev/hda7 zufall	Fügt der verschlüsselten Partition (hda7) einen weiteren Key hinzu. Dieser Key wird aus der Datei zufall gelesen – ist keine Datei angegeben, wird von der Standarteingabe gelesen.
cryptsetup luksDelKey /dev/hda7 1	Löscht den Key mit der ID 1 (VORSICHT! Unbedingt klarheit verschaffen, welcher Key unter der ID 1 geführt wird!)
cryptsetup luksOpen /dev/hda7 mnt --key-file zufall	Öffnet die Partition (hda7) und liest dabei den Key aus der Datei zufall.
cryptsetup luksDump /dev/hda7	Gibt Informationen über die verschlüsselte Partition (hda7) aus.

Links

Dieses Dokument: http://www.sebastianandres.de/vortraege
Cryptsetup Vortrag mit LVM2 Lutz Willek:
https://belug.de/~lutz/pub/vortrag/20060621/LVM2_cryptsetup-Luks.pdf