!!! ACHTUNG - evtl. veraltet - ACHTUNG !!!

Diese Seite wurde zuletzt am 9. Juli 2014 um 10:55 Uhr geändert.

Es gibt unter Linux verschiedene Möglichkeiten, Daten lokal zu verschlüsseln (oder einfach nur zu verstecken).

Welche Lösung zum Einsatz kommt, hängt oft vom Zweck ab:

- möchte ich einfach nur eine Datei verstecken, würde ich cat & split wählen
- möchte ich einfach nur eine Datei verschlüsseln, würde ich mcrypt wählen
- möchte ich einfach nur eine Datei verschlüsseln und verstecken, würde ich steghide wählen
- möchte ich einfach nur ein Verzeichnis verschlüsseln, würde ich EncFs wählen
- möchte ich ganze Festplatten bzw. Partitionen verschlüsseln, würde ich dm-crypt inkl. LUKS wählen
- möchte ich ganze Festplatten bzw. Partitionen verschlüsseln und diese auch unter Mac OS X oder M$ Windoof nutzen, würde ich TrueCrypt wählen
- möchte ich Dateien in der „unallocated area“ oder gar einer HPA verstecken, würde ich doch loop-AES wählen

Da man im Internet immer häufiger über Migrationen von loop-AES nach dm-crypt inkl. LUKS liest, taucht diese Lösung in meiner Auswahl nicht auf.

Was dazu sonst noch so interessant sein könnte:

- Memory-Dump (und mehr... eigentlich eine eigene Seite wert!?)
  - http://ewers.net/llr/
  - Microsoft COFEE (Computer Online Forensic Evidence Extractor)
  - http://www.x-ways.net/capture
  - http://www.storm.net.nz/projects/16
  - http://citp.princeton.edu/memory/
- http://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software
- FileVault (Apple)
- EFS unter windows XP
- Bitlocker (Windows Vista Enterprise and Ultimate)
  - http://www.forensickb.com/2008/01/incident-response-recovering-bitlocker.html
  - http://www.forensickb.com/2008/04/additional-bitlocker-incident-response.html
- DriveCrypt (http://www.securstar.de/)
- SafeGuard (http://www.utimaco.de/)

From:
https://wiki.neumannsland.de/ - **Patricks DokuWiki**

Permanent link:
https://wiki.neumannsland.de/mw2dw:ds3000-verschluesselung

Last update: **2019/09/23 15:08**