

DATEI- UND FESTPLATTENVERSCHLÜSSELUNG MIT TRUECRYPT

„The lesson here is that it is insufficient to protect ourselves with laws;
we need to protect ourselves with mathematics.
Encryption is too important to be left solely to governments.“

Bruce Schneier, 1996

INHALT

- Wieso sollte ich Dateien verschlüsseln?
- Was sollte man beim Verschlüsseln beachten?
- Weshalb sollte ich TrueCrypt einsetzen?
- Wie erstelle ich eine Container-Datei?
- Wie verwende ich eine Container-Datei?
- Wie greife ich unterwegs auf meine Daten zu?

WIESO SOLLTE ICH DATEIEN VERSCHLÜSSELN?

- Schutz vor Diebstahl oder Verlust mobiler Rechner und Datenträger
- Teilen eines Rechners mit weiteren Personen (Familienmitglieder, WG-Mitbewohner, ...)
- Hardware-Reparaturdienste erhalten kaputte Geräte inkl. darauf gespeicherter Daten
- Nutzung eines Cloud-Anbieters

WIESO SOLLTE ICH DATEIEN VERSCHLÜSSELN?

- Problemloser Wiederverkauf eines Datenträgers (Vorsicht bei Flash-Speichern)
- (Unrechtmäßige) Durchsuchungen von Wohnungen oder Smartphones durch Polizeibehörden
- Daten elektronischer Geräte können ohne Verdacht beim Grenzübertritt von Behörden eingesehen und kopiert werden (z.B. USA)

WAS SOLLTE MAN BEIM VERSCHLÜSSELN BEACHTEN?

- Ein laufendes System ist u.a. anfällig für:
 - Ausspähen des Passwortes während der Eingabe (Blick über die Schulter, Überwachungskamera, Keylogger, ...)
 - Ausspionieren von Daten durch Trojaner während der Container entschlüsselt ist
 - Das direkte Auslesen des Schlüssels aus dem Speicher mit Hilfe eines FireWire-Anschlusses
 - Das Auslesen des Schlüssels aus dem Speicher nach Tiefkühlen und Entfernen der RAM-Bausteine



CC0 1.0: FlippyFlink
(Wikimedia)

WAS SOLLTE MAN BEIM VERSCHLÜSSELN BEACHTEN?

- Verschlüsselung steht und fällt mit der Wahl des richtigen Passwortes
 - Zu kurze Passworte lassen sich mittels Brute-Force-Attacke ermitteln
 - Zu einfache sind anfällig für Wörterbuchangriffe
 - Ein sicheres Passwort sollte dennoch merkbar sein
 - Passwortverlust = Datenverlust
 - Niemals unverschlüsselt Passwörter auf der Festplatte ablegen (SpyWare, Trojaner)

WAS SOLLTE MAN BEIM VERSCHLÜSSELN BEACHTEN?

- Zwang zur Herausgabe des Passwortes
 - Erpressung
 - Strafverfolgung (in GB droht Beugehaft, sollte Beweismaterial auf einem verschlüsselten Datenträger vermutet werden)
- Gegenmaßnahme:
Verschlüsselter Container im verschlüsselten Container (Abstreitbarkeit)



WAS SOLLTE MAN BEIM VERSCHLÜSSELN BEACHTEN?

- Datensicherung
 - Ist grundsätzlich sinnvoll ;-)
 - TrueCrypt aktualisiert das Datum des Containers in der Grundeinstellung nicht
 - Backup-Software, die nur das Änderungsdatum einer Datei als Sicherungskriterium verwendet, ignoriert somit den Container
 - Die Windows-Version von TrueCrypt erlaubt es jedoch, das Verhalten zu ändern

WESHALB SOLLTE ICH TRUECRYPT EINSETZEN?

- „Ich bin Windows-Nutzer. Wieso sollte ich nicht EFS (Encrypting File System) oder BitLocker* verwenden?“ (* nur in speziellen Windows-Editionen enthalten)
- „Zum Lieferumfang meines Mac OS X gehört die Verschlüsselungssoftware FileVault. Warum sollte ich diese nicht einsetzen?“
- „Als Linux-User habe ich meine Festplatte mit dm-crypt verschlüsselt. Weshalb sollte ich stattdessen TrueCrypt benutzen?“

WESHALB SOLLTE ICH TRUECRYPT EINSETZEN?

- „Ich bin Windows-Nutzer. Wieso sollte ich nicht EFS (Encrypting File System) oder BitLocker* verwenden?“
(* nur in speziellen Windows-Editionen enthalten)

- „Zum Lieferumfang meines Mac OS X gehört die Verschlüsselungssoftware FileVault. Warum sollte ich diese nicht einsetzen?“

- „Als Linux-User habe ich eine Festplatte mit dm-crypt verschlüsselt. Wieso sollte ich stattdessen TrueCrypt benutzen?“

WESHALB SOLLTE ICH TRUECRYPT EINSETZEN?

- Der Programm-Code von TrueCrypt kann von jedem eingesehen werden (Open Source)
- Fehler, aber auch bewusst platzierte Hintertüren können somit entdeckt werden
- Das Ubuntu Privacy Remix Team hat 2011 eine Sicherheitsanalyse des TrueCrypt 7.0a Codes vorgenommen
- TrueCrypt 7.1a (Windows) wurde nachweislich aus dem öffentlichen Quellcode erstellt

WAS KOMMT NACH TRUECRYPT?

- Die Weiterentwicklung von Truecrypt wurde eingestellt
- Verschiedene Folgeprojekte sind gestartet
- VeraCrypt scheint „das Rennen“ zu machen
- VeraCrypt kann Truecrypt Container öffnen
- Truecrypt kann keine Veracrypt Container lesen