Datentresore mit GNU/Linux

Edgar 'Fast Edi' Hoffmann

Community FreieSoftwareOG

kontakt@freiesoftwareog.org

3. August 2016

Datentresore
Begriffserklärung

Datentresore
Begriffserklärung

Unter einem Datentresor versteht man eine Datei, Partition oder sogar einen ganzen Datenträger, welche durch entsprechende Software verschlüsselt wurde.

Datentresore
Wieso eigentlich?

Datentresore
Wieso eigentlich?

Um einen Datentresor zu verwenden, gibt es viele Gründe:

Datentresore
Wieso eigentlich?

Um einen Datentresor zu verwenden, gibt es viele Gründe:

- Transport von sensiblen Daten auf einem USB-Stick oder einer externen Festplatte

Datentresore
Wieso eigentlich?

Um einen Datentresor zu verwenden, gibt es viele Gründe:

- Transport von sensiblen Daten auf einem USB-Stick oder einer externen Festplatte
- Verschicken von Daten über unsichere Kanäle (Mail, Online-Speicher, etc.)

Datentresore
Wieso eigentlich?

Um einen Datentresor zu verwenden, gibt es viele Gründe:

- Transport von sensiblen Daten auf einem USB-Stick oder einer externen Festplatte
- Verschicken von Daten über unsichere Kanäle (Mail, Online-Speicher, etc.)
- Sichern von Daten, die nicht jeder sehen soll/darf (Mehrbenutzersysteme)

Datentresore - Software CrossCrypt

Datentresore - Software CrossCrypt

- Freie Software (GPL) zur transparenten Ver- und Entschlüsselung

Datentresore - Software CrossCrypt

- Freie Software (GPL) zur transparenten Ver- und Entschlüsselung
- Beherrscht Container-Dateien

Datentresore - Software CrossCrypt

- Freie Software (GPL) zur transparenten Ver- und Entschlüsselung
- Beherrscht Container-Dateien
- Unterstützt die Algorithmen Twofish sowie AES in den Varianten AES-128, AES-192 und AES-256

Datentresore - Software CrossCrypt

- Freie Software (GPL) zur transparenten Ver- und Entschlüsselung
- Beherrscht Container-Dateien
- Unterstützt die Algorithmen Twofish sowie AES in den Varianten AES-128, AES-192 und AES-256
- Kompatibel zu loop-aes und damit eines der wenigen Verschlüsselungsprogramme, die unter GNU/Linux und Windows laufen

Datentresore - Software
CrossCrypt

- Freie Software (GPL) zur transparenten Ver- und Entschlüsselung
- Beherrscht Container-Dateien
- Unterstützt die Algorithmen Twofish sowie AES in den Varianten AES-128, AES-192 und AES-256
- Kompatibel zu loop-aes und damit eines der wenigen Verschlüsselungsprogramme, die unter GNU/Linux und Windows laufen
- Kann verschlüsselte CDs lesen
  ISO-Abbild erzeugen - verschlüsseln - brennen - einhängen

Datentresore - Software
CrossCrypt

- Freie Software (GPL) zur transparenten Ver- und Entschlüsselung
- Beherrscht Container-Dateien
- Unterstützt die Algorithmen Twofish sowie AES in den Varianten AES-128, AES-192 und AES-256
- Kompatibel zu loop-aes und damit eines der wenigen Verschlüsselungsprogramme, die unter GNU/Linux und Windows laufen
- Kann verschlüsselte CDs lesen
  ISO-Abbild erzeugen - verschlüsseln - brennen - einhängen

Datentresore - Software
CrossCrypt

- Freie Software (GPL) zur transparenten Ver- und Entschlüsselung
- Beherrscht Container-Dateien
- Unterstützt die Algorithmen Twofish sowie AES in den Varianten AES-128, AES-192 und AES-256
- Kompatibel zu loop-aes und damit eines der wenigen Verschlüsselungsprogramme, die unter GNU/Linux und Windows laufen
- Kann verschlüsselte CDs lesen
  ISO-Abbild erzeugen - verschlüsseln - brennen - einhängen

FreeOTFE und TrueCrypt benutzen Salt und zufällige Initialisierungsvektoren zur Erhöhung der Sicherheit.
CrossCrypt bietet diese Sicherheit nicht und ist damit anfälliger für Rainbow-Table-Attacken.

Datentresore - Software TrueCrypt/VeraCrypt

Datentresore - Software
TrueCrypt/VeraCrypt

Datentresore - Software TrueCrypt/VeraCrypt

Datentresore - Software TrueCrypt/VeraCrypt

- Basiert auf TrueCrypt 7.1a

Datentresore - Software
TrueCrypt/VeraCrypt

- Basiert auf TrueCrypt 7.1a
- Verschlüsselungs-Algorithmen AES, Serpent und Twofish

Datentresore - Software
TrueCrypt/VeraCrypt

- Basiert auf TrueCrypt 7.1a
- Verschlüsselungs-Algorithmen AES, Serpent und Twofish
- Die Auswahlmöglichkeiten und die theoretische Stärke der Verschlüsselung werden jedoch dadurch erhöht, dass diese Algorithmen miteinander in Kaskaden kombinierbar sind

Datentresore - Software
TrueCrypt/VeraCrypt

- Basiert auf TrueCrypt 7.1a
- Verschlüsselungs-Algorithmen AES, Serpent und Twofish
- Die Auswahlmöglichkeiten und die theoretische Stärke der Verschlüsselung werden jedoch dadurch erhöht, dass diese Algorithmen miteinander in Kaskaden kombinierbar sind
- Für die kryptologischen Hash-Werte stehen RIPEMD-160, SHA-256, SHA-512 und Whirlpool zur Verfügung

Datentresore - Software
TrueCrypt/VeraCrypt

- Basiert auf TrueCrypt 7.1a
- Verschlüsselungs-Algorithmen AES, Serpent und Twofish
- Die Auswahlmöglichkeiten und die theoretische Stärke der Verschlüsselung werden jedoch dadurch erhöht, dass diese Algorithmen miteinander in Kaskaden kombinierbar sind
- Für die kryptologischen Hash-Werte stehen RIPEMD-160, SHA-256, SHA-512 und Whirlpool zur Verfügung
- Verfügbar für GNU/Linux und Windows

Datentresore - Software LibreCrypt

Datentresore - Software LibreCrypt

- Transparente Verschlüsselung

Datentresore - Software LibreCrypt

- Transparente Verschlüsselung
- Container erscheint unter Windows als Laufwerk

Datentresore - Software
LibreCrypt

- Transparente Verschlüsselung
- Container erscheint unter Windows als Laufwerk
- Kompatibel mit GNU/Linux-Verschlüsselung (dm-crypt + LUKS)

Datentresore - Software
LibreCrypt

- Transparente Verschlüsselung
- Container erscheint unter Windows als Laufwerk
- Kompatibel mit GNU/Linux-Verschlüsselung (dm-crypt + LUKS)
- Plausible Abstreitbarkeit

Datentresore - Software
LibreCrypt

- Transparente Verschlüsselung
- Container erscheint unter Windows als Laufwerk
- Kompatibel mit GNU/Linux-Verschlüsselung (dm-crypt + LUKS)
- Plausible Abstreitbarkeit
- Container können auch ohne Admin-Rechte über einen Explorer durchsucht werden

Datentresore - Software
LibreCrypt

- Transparente Verschlüsselung
- Container erscheint unter Windows als Laufwerk
- Kompatibel mit GNU/Linux-Verschlüsselung (dm-crypt + LUKS)
- Plausible Abstreitbarkeit
- Container können auch ohne Admin-Rechte über einen Explorer durchsucht werden
- Smartcards und Sicherheits-Token werden unterstützt

Datentresore - Software
LibreCrypt

- Transparente Verschlüsselung
- Container erscheint unter Windows als Laufwerk
- Kompatibel mit GNU/Linux-Verschlüsselung (dm-crypt + LUKS)
- Plausible Abstreitbarkeit
- Container können auch ohne Admin-Rechte über einen Explorer durchsucht werden
- Smartcards und Sicherheits-Token werden unterstützt
- Die Container können eine Datei, eine Partition oder ein kompletter Datenträger sein

Datentresore - Software
LibreCrypt

- Transparente Verschlüsselung
- Container erscheint unter Windows als Laufwerk
- Kompatibel mit GNU/Linux-Verschlüsselung (dm-crypt + LUKS)
- Plausible Abstreitbarkeit
- Container können auch ohne Admin-Rechte über einen Explorer durchsucht werden
- Smartcards und Sicherheits-Token werden unterstützt
- Die Container können eine Datei, eine Partition oder ein kompletter Datenträger sein
- Unterstützt diverse Hashes und Verschlüsselungs-Algorrhytmen (SHA-512, RIPEMD-320, Tiger / AES, Twofish, Serpent)

Datentresore - Software
LibreCrypt

- Transparente Verschlüsselung
- Container erscheint unter Windows als Laufwerk
- Kompatibel mit GNU/Linux-Verschlüsselung (dm-crypt + LUKS)
- Plausible Abstreitbarkeit
- Container können auch ohne Admin-Rechte über einen Explorer durchsucht werden
- Smartcards und Sicherheits-Token werden unterstützt
- Die Container können eine Datei, eine Partition oder ein kompletter Datenträger sein
- Unterstützt diverse Hashes und Verschlüsselungs-Algorrhytmen (SHA-512, RIPEMD-320, Tiger / AES, Twofish, Serpent)
- Mit einer optionalen 'Schlüsseldatei" kann ein USB-Stick als Schlüssel verwendet werden

Datentresore - Software
LibreCrypt

- Transparente Verschlüsselung
- Container erscheint unter Windows als Laufwerk
- Kompatibel mit GNU/Linux-Verschlüsselung (dm-crypt + LUKS)
- Plausible Abstreitbarkeit
- Container können auch ohne Admin-Rechte über einen Explorer durchsucht werden
- Smartcards und Sicherheits-Token werden unterstützt
- Die Container können eine Datei, eine Partition oder ein kompletter Datenträger sein
- Unterstützt diverse Hashes und Verschlüsselungs-Algorrhytmen (SHA-512, RIPEMD-320, Tiger / AES, Twofish, Serpent)
- Mit einer optionalen 'Schlüsseldatei" kann ein USB-Stick als Schlüssel verwendet werden
- Kann portabel verwendet werden (benötigt allerdings Admin-Rechte)

Datentresore - Software
LibreCrypt

- Transparente Verschlüsselung
- Container erscheint unter Windows als Laufwerk
- Kompatibel mit GNU/Linux-Verschlüsselung (dm-crypt + LUKS)
- Plausible Abstreitbarkeit
- Container können auch ohne Admin-Rechte über einen Explorer durchsucht werden
- Smartcards und Sicherheits-Token werden unterstützt
- Die Container können eine Datei, eine Partition oder ein kompletter Datenträger sein
- Unterstützt diverse Hashes und Verschlüsselungs-Algorrhytmen (SHA-512, RIPEMD-320, Tiger / AES, Twofish, Serpent)
- Mit einer optionalen 'Schlüsseldatei" kann ein USB-Stick als Schlüssel verwendet werden
- Kann portabel verwendet werden (benötigt allerdings Admin-Rechte)
- Leider nur für Windows verfügbar

Datentresore - Software
DM-Crypt + LUKS

Datentresore - Software
DM-Crypt + LUKS

dm-crypt + LUKS ist die native GNU/Linux Disk-Verschlüsselung vieler Distributionen.

Datentresore - Software
DM-Crypt + LUKS

dm-crypt + LUKS ist die native GNU/Linux Disk-Verschlüsselung vieler Distributionen.
Ausserdem bedeutet es: **L**inux **U**nified **K**ey **S**etup

Datentresore - Software
DM-Crypt + LUKS

Datentresore - Software
DM-Crypt + LUKS

- Verfügbar für Windows, GNU/Linux (nativ), Android (nur BS)

Datentresore - Software
DM-Crypt + LUKS

- Verfügbar für Windows, GNU/Linux (nativ), Android (nur BS)
- Unterstützte Verschlüsselung: AES-256, weitere können hineinkompiliert werden

Datentresore - Software
DM-Crypt + LUKS

- Verfügbar für Windows, GNU/Linux (nativ), Android (nur BS)
- Unterstützte Verschlüsselung: AES-256, weitere können hineinkompiliert werden
- Verschlüsselungsschicht: Block-Level, kann verschiedene Dateisysteme enthalten

Datentresore - Software
DM-Crypt + LUKS

- Verfügbar für Windows, GNU/Linux (nativ), Android (nur BS)
- Unterstützte Verschlüsselung: AES-256, weitere können hineinkompiliert werden
- Verschlüsselungsschicht: Block-Level, kann verschiedene Dateisysteme enthalten
- Lizenz: GPL

Datentresore - Software zuluCrypt

Datentresore - Software
zuluCrypt

Datentresore - Software zuluCrypt

Datentresore - Software zuluCrypt

- Verschlüsselung einzelner Dateien, Container und Partitionen

Datentresore - Software zuluCrypt

- Verschlüsselung einzelner Dateien, Container und Partitionen
- versteht die linuxspezifische Verschlüsselungsmethode LUKS und vereinfacht deren Nutzung über schlichte Menüs

Datentresore - Software zuluCrypt

- Verschlüsselung einzelner Dateien, Container und Partitionen
- versteht die linuxspezifische Verschlüsselungsmethode LUKS und vereinfacht deren Nutzung über schlichte Menüs
- (Front-End für die Tools tcplay und cryptsetup)

Datentresore - Software zuluCrypt

- Verschlüsselung einzelner Dateien, Container und Partitionen
- versteht die linuxspezifische Verschlüsselungsmethode LUKS und vereinfacht deren Nutzung über schlichte Menüs
- (Front-End für die Tools tcplay und cryptsetup)
- Als Safe für Passwörter kann der Gnome-Keyring (Gnome/Unity) dienen und in KDE der sichere Kennwortspeicher Kwallet

Datentresore - Software zuluCrypt

- Verschlüsselung einzelner Dateien, Container und Partitionen
- versteht die linuxspezifische Verschlüsselungsmethode LUKS und vereinfacht deren Nutzung über schlichte Menüs
- (Front-End für die Tools tcplay und cryptsetup)
- Als Safe für Passwörter kann der Gnome-Keyring (Gnome/Unity) dienen und in KDE der sichere Kennwortspeicher Kwallet
- Einfache grafische Oberfläche, kann jedoch auch auf der Konsole bedient werden

Datentresore - Software zuluCrypt

- Verschlüsselung einzelner Dateien, Container und Partitionen
- versteht die linuxspezifische Verschlüsselungsmethode LUKS und vereinfacht deren Nutzung über schlichte Menüs
- (Front-End für die Tools tcplay und cryptsetup)
- Als Safe für Passwörter kann der Gnome-Keyring (Gnome/Unity) dienen und in KDE der sichere Kennwortspeicher Kwallet
- Einfache grafische Oberfläche, kann jedoch auch auf der Konsole bedient werden
- Lizenz: BSD

Datentresore - Software Tomb

Datentresore - Software Tomb

Datentresore - Software Tomb

Datentresore - Software
Tomb

Tomb ist Freie Software zur Verschlüsselung von Dateien unter GNU/Linux und möchte die Sicherung von geheimen Daten vereinfachen.

Datentresore - Software
Tomb

Tomb ist Freie Software zur Verschlüsselung von Dateien unter GNU/Linux und möchte die Sicherung von geheimen Daten vereinfachen.
Funktionen von Tomb:

Datentresore - Software Tomb

Tomb ist Freie Software zur Verschlüsselung von Dateien unter GNU/Linux und möchte die Sicherung von geheimen Daten vereinfachen.
Funktionen von Tomb:

- Erstellung von verschlüsselten Containern

Datentresore - Software
Tomb

Tomb ist Freie Software zur Verschlüsselung von Dateien unter GNU/Linux und möchte die Sicherung von geheimen Daten vereinfachen.
Funktionen von Tomb:

- Erstellung von verschlüsselten Containern
- Erstellung von einer separaten Schlüsseldatei, mit zusätzlicher Sicherung durch ein Passwort

Datentresore - Software
Tomb

Tomb ist Freie Software zur Verschlüsselung von Dateien unter GNU/Linux und möchte die Sicherung von geheimen Daten vereinfachen.
Funktionen von Tomb:

- Erstellung von verschlüsselten Containern
- Erstellung von einer separaten Schlüsseldatei, mit zusätzlicher Sicherung durch ein Passwort
- Schlüsseldatei kann mittels Steganographie in einem Bild versteckt/transportiert werden (steghide)

Datentresore - Begrifflichkeit
Glaubhafte Abstreitbarkeit

Datentresore - Begrifflichkeit
Glaubhafte Abstreitbarkeit

Glaubhafte Abstreitbarkeit (auch glaubhafte Bestreitbarkeit; englisch plausible deniability) ist ein Konzept zum Vermeiden von Spuren, die einen Sachverhalt forensisch nachweisbar machen. Im besten Fall wird sogar ein plausibles Alibi geschaffen.

Datentresore - Begrifflichkeit
Glaubhafte Abstreitbarkeit

Glaubhafte Abstreitbarkeit (auch glaubhafte Bestreitbarkeit; englisch plausible deniability) ist ein Konzept zum Vermeiden von Spuren, die einen Sachverhalt forensisch nachweisbar machen. Im besten Fall wird sogar ein plausibles Alibi geschaffen.

In der Informationstechnik werden Mechanismen zur glaubhaften Abstreitbarkeit bei anonymen Peer-to-Peer-Netzen oder generell bei Datenverschlüsselung eingesetzt, um den Ursprung oder das Vorhandensein von Informationen abstreiten zu können.

Datentresore - Begrifflichkeit
Glaubhafte Abstreitbarkeit

Glaubhafte Abstreitbarkeit (auch glaubhafte Bestreitbarkeit; englisch plausible deniability) ist ein Konzept zum Vermeiden von Spuren, die einen Sachverhalt forensisch nachweisbar machen. Im besten Fall wird sogar ein plausibles Alibi geschaffen.

In der Informationstechnik werden Mechanismen zur glaubhaften Abstreitbarkeit bei anonymen Peer-to-Peer-Netzen oder generell bei Datenverschlüsselung eingesetzt, um den Ursprung oder das Vorhandensein von Informationen abstreiten zu können.

Es sind Verfahren, um vertrauliche Daten oder den Ursprung von Daten zu verbergen, so dass deren Existenz oder Ursprung nicht nachgewiesen werden kann.

Datentresore - Begrifflichkeit
Glaubhafte Abstreitbarkeit

Glaubhafte Abstreitbarkeit (auch glaubhafte Bestreitbarkeit; englisch plausible deniability) ist ein Konzept zum Vermeiden von Spuren, die einen Sachverhalt forensisch nachweisbar machen. Im besten Fall wird sogar ein plausibles Alibi geschaffen.

In der Informationstechnik werden Mechanismen zur glaubhaften Abstreitbarkeit bei anonymen Peer-to-Peer-Netzen oder generell bei Datenverschlüsselung eingesetzt, um den Ursprung oder das Vorhandensein von Informationen abstreiten zu können.

Es sind Verfahren, um vertrauliche Daten oder den Ursprung von Daten zu verbergen, so dass deren Existenz oder Ursprung nicht nachgewiesen werden kann.

Bekannte, aktuelle Beispiele sind das anonyme, zensurresistente Netz Tor und Freenet und die Dateiverschlüsselungssoftware FreeOTFE und TrueCrypt/VeraCrypt.

Datentresore - Begrifflichkeit
Glaubhafte Abstreitbarkeit

Glaubhafte Abstreitbarkeit (auch glaubhafte Bestreitbarkeit; englisch plausible deniability) ist ein Konzept zum Vermeiden von Spuren, die einen Sachverhalt forensisch nachweisbar machen. Im besten Fall wird sogar ein plausibles Alibi geschaffen.

In der Informationstechnik werden Mechanismen zur glaubhaften Abstreitbarkeit bei anonymen Peer-to-Peer-Netzen oder generell bei Datenverschlüsselung eingesetzt, um den Ursprung oder das Vorhandensein von Informationen abstreiten zu können.

Es sind Verfahren, um vertrauliche Daten oder den Ursprung von Daten zu verbergen, so dass deren Existenz oder Ursprung nicht nachgewiesen werden kann.

Bekannte, aktuelle Beispiele sind das anonyme, zensurresistente Netz Tor und Freenet und die Dateiverschlüsselungssoftware FreeOTFE und TrueCrypt/VeraCrypt.

Auch das Verschlüsselungsprinzip des Off-the-Record Messaging (OTR) gewährleistet die glaubhafte Abstreitbarkeit.

Datentresore - Begrifflichkeit
Glaubhafte Abstreitbarkeit

Datentresore - Begrifflichkeit
Glaubhafte Abstreitbarkeit

Hierunter wird ein innerhalb eines anderen Containers verstecktes virtuelles Laufwerk verstanden, das mit Hilfe eines separaten Passwortes entsperrt werden muss.

Datentresore - Begrifflichkeit
Glaubhafte Abstreitbarkeit

Hierunter wird ein innerhalb eines anderen Containers verstecktes virtuelles Laufwerk verstanden, das mit Hilfe eines separaten Passwortes entsperrt werden muss.

Standardmäßig wird freier Speicherplatz eines regulären Containers mit zufälligen Daten aufgefüllt.
In diesem freien Bereich wird (z.B. von VeraCrypt) der etwaige versteckte Container gespeichert.

Datentresore - Begrifflichkeit
Glaubhafte Abstreitbarkeit

Hierunter wird ein innerhalb eines anderen Containers verstecktes virtuelles Laufwerk verstanden, das mit Hilfe eines separaten Passwortes entsperrt werden muss.

Standardmäßig wird freier Speicherplatz eines regulären Containers mit zufälligen Daten aufgefüllt.
In diesem freien Bereich wird (z.B. von VeraCrypt) der etwaige versteckte Container gespeichert.

Für einen außenstehenden Betrachter ist nicht erkennbar, ob es sich bei einem Bereich eines Containers um überschriebenen freien Speicherplatz oder einen versteckten Container handelt.

Datentresore - Begrifflichkeit
Glaubhafte Abstreitbarkeit

Datentresore - Begrifflichkeit
Glaubhafte Abstreitbarkeit

Der äußere und der darin versteckte Container sind jeweils mit einem separaten Passwort zugänglich.
Je nachdem, welches der beiden Passwörter eingegeben wird, wird der jeweilige Container entsperrt.

Datentresore - Begrifflichkeit
Glaubhafte Abstreitbarkeit

Der äußere und der darin versteckte Container sind jeweils mit einem separaten Passwort zugänglich.
Je nachdem, welches der beiden Passwörter eingegeben wird, wird der jeweilige Container entsperrt.

Hierdurch können Anwender, wenn sie beispielsweise von den Behörden zur Herausgabe des Passwortes aufgefordert werden, weniger sensible Daten durch Eintippen des Passwortes für den äußeren Container preisgeben, ohne dass hierdurch die sensibleren Daten im versteckten Container erkennbar werden.

Datentresore - Begrifflichkeit
Glaubhafte Abstreitbarkeit

Der äußere und der darin versteckte Container sind jeweils mit einem separaten Passwort zugänglich.
Je nachdem, welches der beiden Passwörter eingegeben wird, wird der jeweilige Container entsperrt.

Hierdurch können Anwender, wenn sie beispielsweise von den Behörden zur Herausgabe des Passwortes aufgefordert werden, weniger sensible Daten durch Eintippen des Passwortes für den äußeren Container preisgeben, ohne dass hierdurch die sensibleren Daten im versteckten Container erkennbar werden.

Da für einen Angreifer nicht erkennbar ist, dass ein versteckter Container genutzt wurde, blieben hierdurch die Daten geschützt.

Datentresore - Steganographie
Ausblick auf ein neues Thema

Datentresore - Steganographie
Ausblick auf ein neues Thema

Eine weitere Möglichkeit, Daten zu verstecken bzw. zu verschlüsseln ist die sogenannte Steganographie, d.h. Daten werden in unverfänglichen anderen Daten versteckt.

Hands-On
Mit Tomb

Hands-On
Mit Tomb

D E M O

Links zur Präsentation

https://veracrypt.codeplex.com/
https://www.dyne.org/software/tomb/
http://mhogomchungu.github.io/zuluCrypt/
https://github.com/t-d-k/LibreCrypt

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 und Thema laut Webseite)

FreieSoftwareOG.org