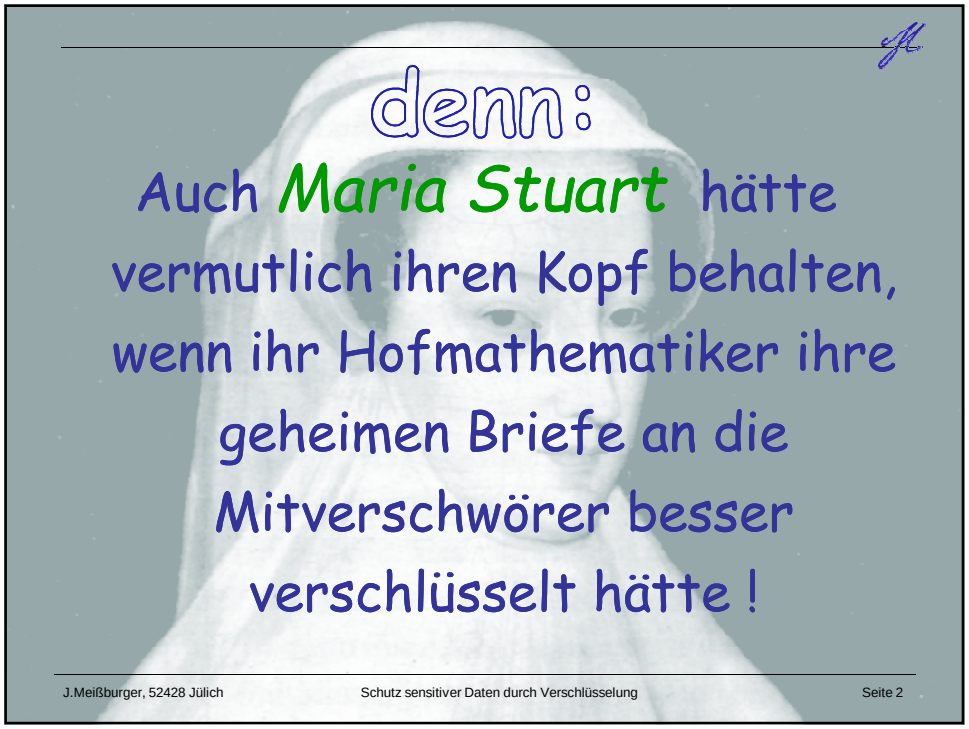
Nur nicht den Kopf verlieren ....

Schutz durch starke Datenverschlüsselung



deshalb:

- Entscheidende Kriterien für die Sicherheit einer Verschlüsselung sind:
- Die Stärke der Verschlüsselung.
  - = verwendeter Algorithmus
- Die Güte der verwendeten Schlüssel.
  - = Länge und Komplexität der Passwörter
- Und nicht zu vergessen:
  - Ein Schlüssel in fremder Hand oder ein verlorener Schlüssel kosten vielleicht nicht den Kopf, aber ….

J.Meißburger, 52428 Jülich Schutz sensitiver Daten durch Verschlüsselung Seite 3

Thema „Datensicherheit"

1. Sicherstellen der Daten-Verfügbarkeit:
   Thema: „Datensicherung, Backup" – früher !
1. Schutz vor unautorisierter und meist unbemerkter Veränderung der Daten, Daten-Integrität:
   Thema: „Digitale Signatur" – vielleicht demnächst ?
2. Schutz der Daten vor fremdem, nicht-autorisiertem Lese-Zugriff, Wahrung der Daten-Vertraulichkeit:
   Thema: „Verschlüsselung" – heute!

J.Meißburger, 52428 Jülich Schutz sensitiver Daten durch Verschlüsselung Seite 4

Grundsätzliches:

- Prinzipiell ist keine konventionelle Verschlüsselung zu 100% sicher!
- Sie gilt als „sicher“, wenn man zu ihrer Entschlüsselung auf den schnellsten Rechnern der Welt (Tianhe-2 33.86 PetaFLOP LinPack = 33.860.000.000.000.000 Rechenoperationen/sec)

  Tausende von Jahren benötigen würde.
- Prinzipiell 100% sicher ist nur die in Entwicklung befindliche Quantenkryptographie.
- Neueste Entwicklungen („D-Wave“) zur Daten-Entschlüsselung nutzen Quanten-Computing.

J.Meißburger, 52428 Jülich Schutz sensitiver Daten durch Verschlüsselung Seite 5

was muss verschlüsselt werden ?

- Ganze Verzeichnisse, Partitionen oder Datenträger (USB-Stick!) mit sensitiven Daten.
- Email auf dem Weg vom und zum Mailserver inklusive Mail-Inhalt und Anhängen.
- Master-Passwörter, Zugangs-Passwörter, PIN‘s, Kryptographie-Schlüssel, Zertifikate.
- Datenkommunikation mit Webservern, vor allem beim Ausfüllen sensitiver Formulare (https).
- Kommunikation im Funknetz (WiFi - WPA2).
- Private Datenkommunikation über öffentliche Netze (Virtual Private Networks).

J.Meißburger, 52428 Jülich Schutz sensitiver Daten durch Verschlüsselung Seite 6

einige Tipps für die Praxis

- „Normale“ Passwörter mindestens ≥12 Zeichen lang und komplex (Buchstaben klein/groß, Zahlen, Leerzeichen, Sonderzeichen).
- WPA2-Schlüssel und Master-Passwörter komplex und mindestens ***21*** Zeichen lang
- Bei Web-Formularen immer auf https: bzw. Schloss-Symbol achten.
- Bei Verwendung von Email-Klienten (Outlook, Windows Mail, Thunderbird etc.) immer die Serverports auf gesicherte Kommunikation (SSL/TLS) in beiden Richtungen einstellen.

J.Meißburger, 52428 Jülich Schutz sensitiver Daten durch Verschlüsselung Seite 7

Gute Passwörter

- Keine Namen oder Begriffe, die man in irgendeinem Wörterbuch oder Lexikon finden kann (vor allem keine Eigennamen).
- Keine Fachbegriffe, egal aus welcher Branche
- Groß- und Kleinschreibung, Sonderzeichen, Leerzeichen und Ziffern verwenden.
- Keine „national characters“ (ä,ö,ü,ß,é,â, etc.) benutzen oder zumindest vorher testen!
- Passwort (immer verändert) überprüfen unter http://www.passwordmeter.com

J.Meißburger, 52428 Jülich Schutz sensitiver Daten durch Verschlüsselung Seite 8

Verschlüsselungsverfahren

- Symmetrische Verschlüsselung:
  Sender und Empfänger kennen ein gemeinsam verwendetes Passwort (Schlüssel) zum Ver- und Entschlüsseln.
- Unsymmetrische Verschlüsselung: Der Sender besitzt einen geheimen, privaten Schlüssel und sendet einen zweiten, „öffentlichen“ Schlüssel an den Empfänger. Dieser kann damit Daten an den Sender verschlüsseln, die nur dieser mit seinem privaten Schlüssel entschlüsseln kann.

Software für die symmetrische Verschlüsselung

- **Ordner-Verschlüsselung Windows**
  - nur NTFS-Dateisystem ab Windows XP. Nur Windows Pro/Enterprise/Ultimate.
- **TrueCrypt**
  - Krypto-Container als virtuelle Laufwerke mit speziellem Treiber, deshalb so einfach und schnell wie normale Windows-Ordner zu benutzen.
- **PrivateCrypto**
  - verschlüsselt Ordner und Dateien in selbst-extrahierende Krypto-Dateien mit Selbstschutz.

TrueCrypt
das „Schweizer Messer" der Verschlüsselung

- Verschlüsselt Dateien, Ordner mit Unterordnern oder ganze Partitionen bzw. Laufwerke.
- Ist sehr komfortabel mit Hotkeys zu benutzen.
- Benutzt bewährte und standardisierte, sichere Verschlüsselungsverfahren.
- Ist unter GNU Public License entwickelt (Quellcode-offen) und millionenfach im Einsatz.
- Hinterlässt auch bei Unachtsamkeit keine unverschlüsselten Daten auf dem PC!

TrueCrypt installieren

- Herunterladen von "truecrypt_setup_x.x.exe" von www.truecrypt.org/downloads
- Durch Doppelklick installieren, Benutzerkonten-Steuerung bestätigen (Treiberinstallation!)
- Language-Pack Deutsch herunterladen: „langpack-de-X.X.X-for-truecrypt-X.Xx.zip"
- Extrahieren mit RM und „Language.de.xml" ins Installationsverzeichnis unter C:\Programme\TrueCrypt (64bit) oder C:\Programme (x86)\TrueCrypt kopieren
- TrueCrypt (neu) starten
- Falls die Sprache nicht automatisch erkannt wurde, mit „Einstellungen – Sprache" Deutsch auswählen

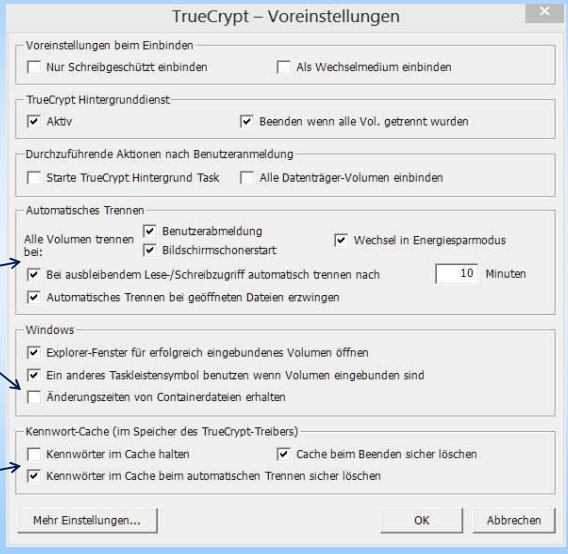
Einstellungen - Voreinstellungen

Sicherheit bei Inaktivität:

immer trennen, wenn inaktiv

Änderungsdatum aktualisieren

Cache immer löschen



J.Meißburger, 52428 Jülich Schutz sensitiver Daten durch Verschlüsselung Seite 13

Tastaturkürzel (hotkeys)

- Zum schnellen Starten des Programms:

❖ TrueCrypt-Icon – Rechte Maustaste – Eigenschaften:

❖ STRG+ALT+T als Schnellstart einrichten

J.Meißburger, 52428 Jülich Schutz sensitiver Daten durch Verschlüsselung Seite 14

Zum Öffnen & Schließen von Crypto-Containern (Volumes)

- Einstellungen – Tastenkombinationen:

CTRL-ALT-M öffnet (mounted) alle Favoriten-Volumes

CTRL-ALT-U schließt alle Volumes und löscht alle Caches

Krypto-Container erstellen

- TrueCrypt starten
  - Volumen – Neues Volumen erstellen
  - Eine verschlüsselte Containerdatei erstellen
  - Standard TrueCrypt-Volumen
  - Volumen-Speicherort – Datei
    - Dateinamen und Verzeichnis – nur ASCII – angeben und Verschlüsselungseinstellungen akzeptieren
  - Volumen-Größe z.B. 256 MB
  - Volumen-Kennwort: Gute Passphrase (> 20 ASCII-Zeichen, keine Umlaute oder „ß“ ☹)
  - Als Administrator evtl. NTFS, sonst FAT wählen
  - Formatieren – Benutzerkontensteuerung bestätigen

Verwendung unter Android?

- Mit EDS Lite (kostenlos) bzw. mit EDS pro lassen sich die Krypto-Container auch unter Android erstellen, öffnen und beschreiben.
- Dafür sind folgende Einstellungen bindend:
  1. Verschlüsselungsverfahren AES
  2. Hash Algorithmus 512 bit SHA-512
  3. Volume-Format FAT
- Vorsicht: Wer den Container in der Cloud (SkyDrive, GoogleDrive, Dropbox) ablegen will, sollte nochmal nachdenken und ein sehr gutes Passwort (!!!) verwenden!

Container benutzen

- TrueCrypt starten – Datei
- Krypto-Container auswählen – Einbinden
- Passwort eingeben: Der Container wird als neues Windows-Laufwerk (z.B. „S“) angezeigt.
- Mit diesem Laufwerk kann nun wie mit jedem anderen Windows-Ordner gearbeitet werden, d.h. es können Dateien und Ordner erstellt, kopiert, gelöscht oder verschoben werden.
- Auf Wunsch: Favoriten – Eingebundenes Volumen hinzufügen
- Zum Schluss einfach mit <Strg>-U oder mit „Alle trennen“ den Container wieder schließen

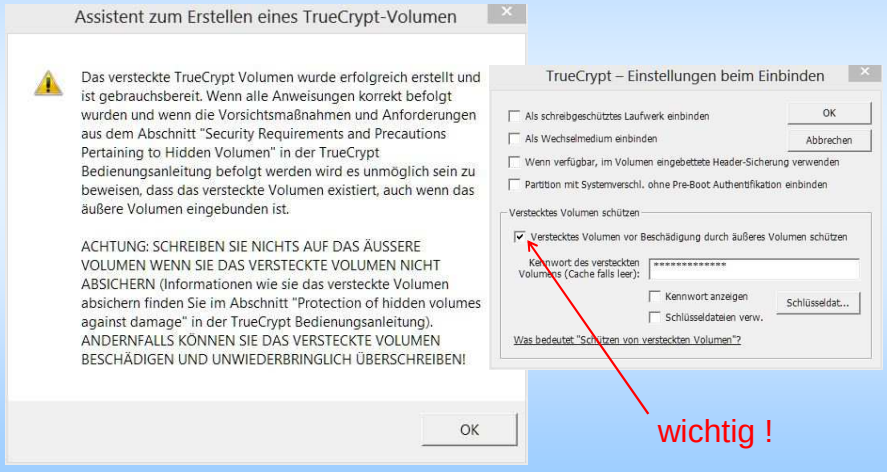
weitere Schutzmechanismen

- Prinzip: *Was der Datendieb nicht weiß, macht ihn nicht heiß!*
- Verfahren 1: Hidden Volumes
  - das sind Krypto-Container, die unsichtbar in anderen Krypto-Containern versteckt sind.
  - In dem scheinbar willkürlichen Gemisch aus Nullen und Einsen ist dies nicht feststellbar.
  - Träger-Container und versteckter Container werden mit unterschiedlichem Passwörtern geöffnet.

Hidden Container erstellen

- TrueCrypt starten (Container nicht einbinden!)
- Extras - TrueCrypt-Volumen erstellen
- Eine verschlüsselte Containerdatei erstellen
- Verstecktes TrueCrypt-Volumen
- Direkter Modus
- Vorhandenen TrueCrypt-Container als Volumen-Speicherort auswählen
- Passwort für vorhandenen Container eingeben
- Größe und Passwort für das neue, versteckte Volumen innerhalb des Containers eingeben

Unbedingt: Hidden Container gegen Überschreiben schützen!



weitere Schutzmechanismen

- Verfahren 2: Steganografie
  1. Dabei werden beliebige Daten verschlüsselt und so in großen Multimedia-Dateien verteilt, dass die Bild- oder Tonveränderungen auch bei hoher Auflösung nicht feststellbar sind.
  2. Im Gegensatz zu hidden volumes kann die Veränderung aber mit mathematischen Verfahren erkannt werden.
  3. Der Inhalt selbst ist aber verschlüsselt und nur mit Passwort zugänglich.

Zum Thema Steganographie:

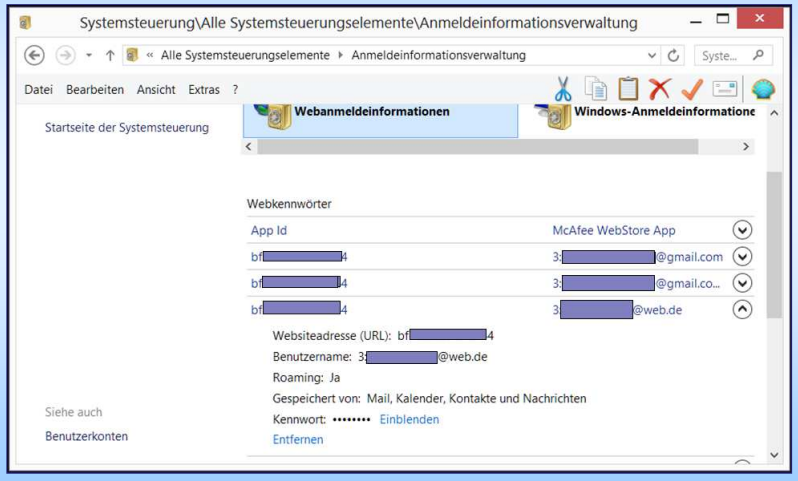
Password-Tresore

wohin mit den Passwörtern ???

- Zur verschlüsselten Speicherung von Zugangsdaten wie URL, Benutzername und Passwort.
- Sicherung durch Master-Passwort und auf Wunsch durch eine Schlüsseldatei (keyfile).
- Automatische und sichere Übertragung der Login-Informationen in Web-Formulare.
- Anschlagsequenz für jeden Webserver separat einstellbar (programmierbar durch Skript)

Windows Systemsteuerung

- „Eigene Anmeldeinformationen verwalten“



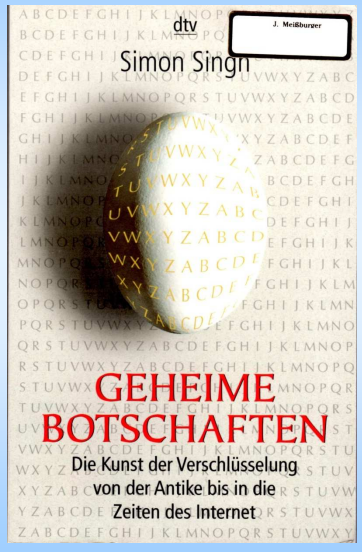
KeePass Password-Safe

- Verschlüsselte Datenbank für Passwörter mit automatischer Übertragung in Web-Formulare

Nützliche Links zu TrueCrypt

- http://www.truecrypt.org/downloads
- http://www.datenschutz.rlp.de/de/selbstds.php?submenu=cloud&prod=truecrypt
- https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Datenverschluesselung/Praxis/Software/software_node.html
- http://de.wikipedia.org/wiki/TrueCrypt

Spannende Lektüre zum Thema:



- Ein spannendes Buch zur Geschichte der Verschlüsselung
- im Deutschen Taschenbuchverlag dtv
- ISBN 3-446-19873-3