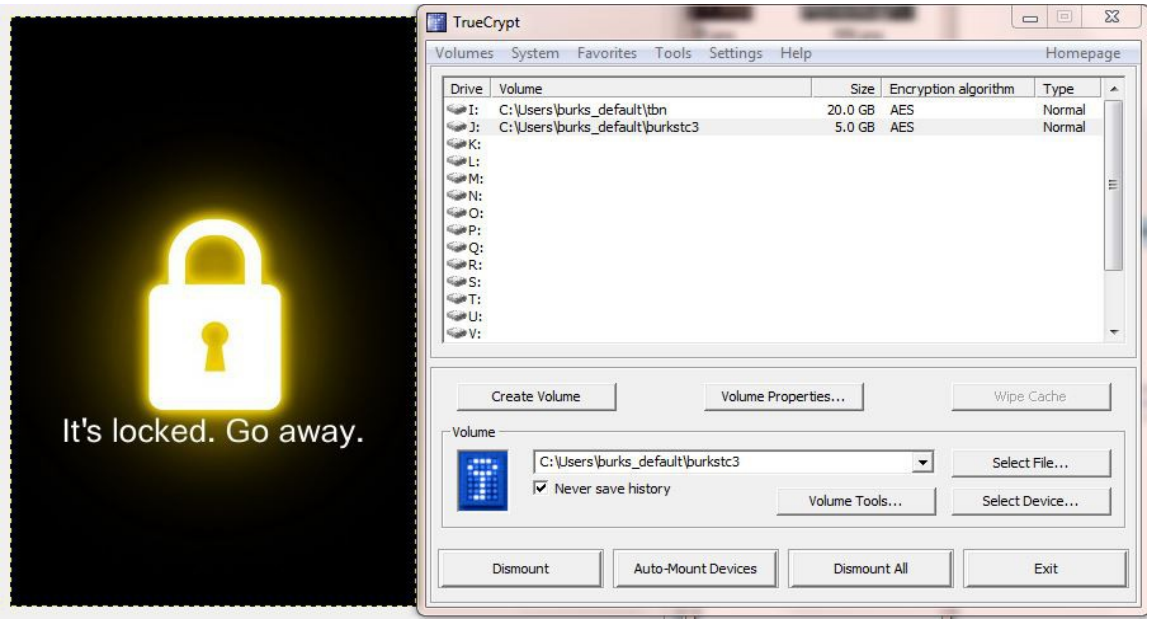
Modul: Sichere Daten

Sicherheit zuhause und unterwegs: Daten sicher verwalten auf dem eigenen Rechner (u.a. mit Truecrypt) und auf fremden Rechnern
Sicherheitsrisiken bei Smartphones



Definition:

Vertrauliche Daten auf Ihren Rechnern (Computer, USB-Sticks, externe Festplatten, Smartphones) gehören in geschützte Truecrypt-Container, anderenfalls handeln Sie unprofessionell und fahrlässig.

“Vertrauliche” Daten sind *alle* Daten, die
- Sie nicht im Internet publizieren würden,
- Sie nicht als Postkarte verschicken würden,
- die Sie als “privat” definieren,
- die Ihnen von anderen anvertraut wurden.

Risiken 1

- Ihre E-Mails werden abgehört (geregelt durch die TKÜV), Ihre Kontakt- und Kommunikationsdaten werden anlasslos gespeichert. Vgl. die aktuellen Medienberichte, z.B.:

- PRISM (Apronym für „Planning Tool for Resource Integration, Synchronization, and Management“, ergibt englisch prism „Prisma“) ist ein seit 2005 existierendes, als streng geheim eingestuftes und von der US-amerikanischen National Security Agency (NSA) geführtes Programm zur Überwachung und Auswertung von elektronischen Medien und elektronisch gespeicherten Daten.

Laut einer zuerst von der US-amerikanischen Washington Post und dem britischen Guardian im Juni 2013 veröffentlichten Präsentation sind an dem Programm neun der größten Internetkonzerne und Dienste der USA beteiligt: Microsoft (u.a. mit Skype), Google (u. a. mit YouTube), Facebook, Yahoo!, Apple, AOL und PalTalk.

PRISM soll eine umfassende Überwachung von Personen innerhalb und außerhalb der USA ermöglichen, die digital kommunizieren.

- Zeit online (21.03.2013): “Bundestag erlaubt Polizei Abfrage von PIN und Passwörtern“

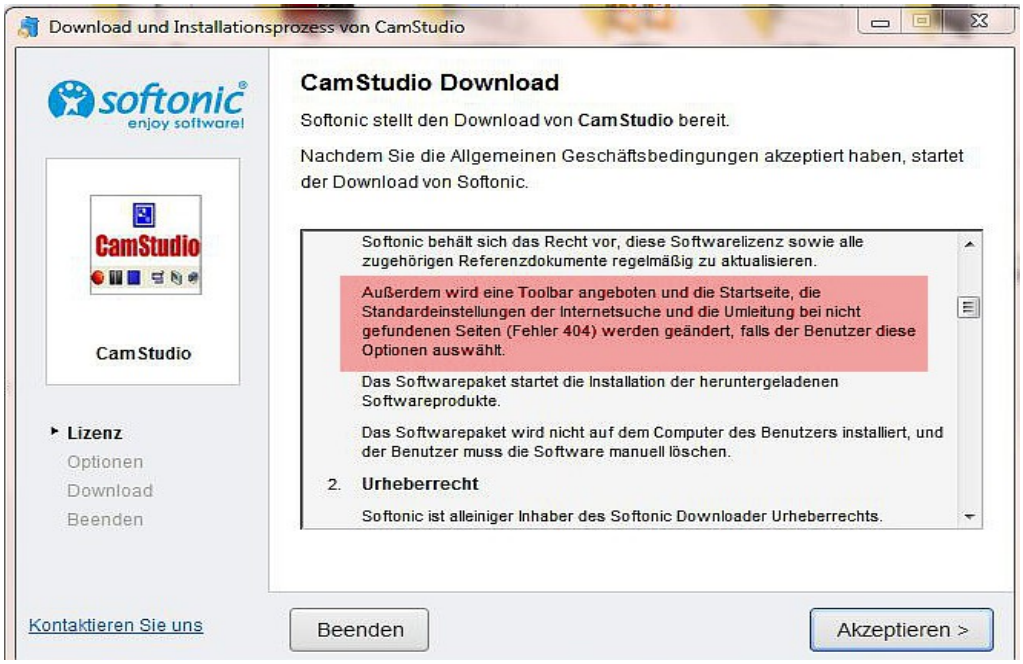
Welche Konsequenzen ziehen Sie persönlich und für diejenigen, mit denen Sie kommunizieren?

Können unbefugte Personen auf Ihre Rechner und Daten zugreifen? (Diebstahl, Beschlagnahmung, Arbeitskollegen)

Ein Sicherheitskonzept umfasst:

Sicherheit der Daten auf Rechnern
Sichere USB-Sticks und externe Festplatten / Backups
Höchste Ansprüche an Cloud-Anbieter

Konsequent sicherheitsbewusstes Verhalten beim E-Mailen und Surfen
Höchste Vorsicht beim Installieren von Software



Truecrypt

Will TrueCrypt be open-source and free forever?
Yes, it will. We will never create a commercial version of TrueCrypt, as we believe in open-source and free security software.

1. Zum Üben

Truecrypt installieren und einen kleinen Container zum Üben einrichten - dieser wird von Ihrem Rechner als normaler Dateiordner behandelt und kann jederzeit gelöscht werden. Ist der Container geschlossen (nicht "gemountet"), erscheint er als eine "Datei" (mit der Dateiendung.tc)

Probieren Sie das auf ihrem Rechner und auf einem leeren USM-Stick.

2. Schritt

Erzeugen Sie Truecypt-Container und machen Sie diese ausreichend groß. (Thunderbird z.B. sollte mindestens 1 Gigybyte zur Verfügung haben.) Schieben Sie die Dateien und Dateiordner, die Sie zukünftig als vertraulich behandeln wollen, einfach in die jeweiligen Container.
Legen Sie eine Verknüpfung auf dem Desktop an (optional).

Verständliche Anleitungen:

Bundesamt für Sicherheit in der Informationstechnik (BSI): Verschlüsselung mit Software
https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Datenverschluesselung/Praxis/Software/software_node.html

Computerbild: Truecrypt - Private Dateien auf Festplatte und USB-Stick schützen
http://www.computerbild.de/artikel/cb-Downloads-Sicherheit-Datenschutz-TrueCrypt-Tipps-Anleitung-5545517.html

Universität Tübingen - Juristische Fakultät: Anleitung zur Verschlüsselung von Datenträgern mit TrueCrypt (sehr verständlich)
http://www.jura.uni-tuebingen.de/einrichtungen/cz/veranstaltungen/TrueCrypt.pdf

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Kurzanleitung TrueCrypt (deutshe Anleitung, englische Sceenshots)
https://www.datenschutzzentrum.de/schule/kurzanleitung-truecrypt-hd.pdf

Truecrypt-Tutorial (Englisch, alles inklusive, 19 Schritte, mit ausagekräftigen Screenshots)
http://www.truecrypt.org/docs/tutorial

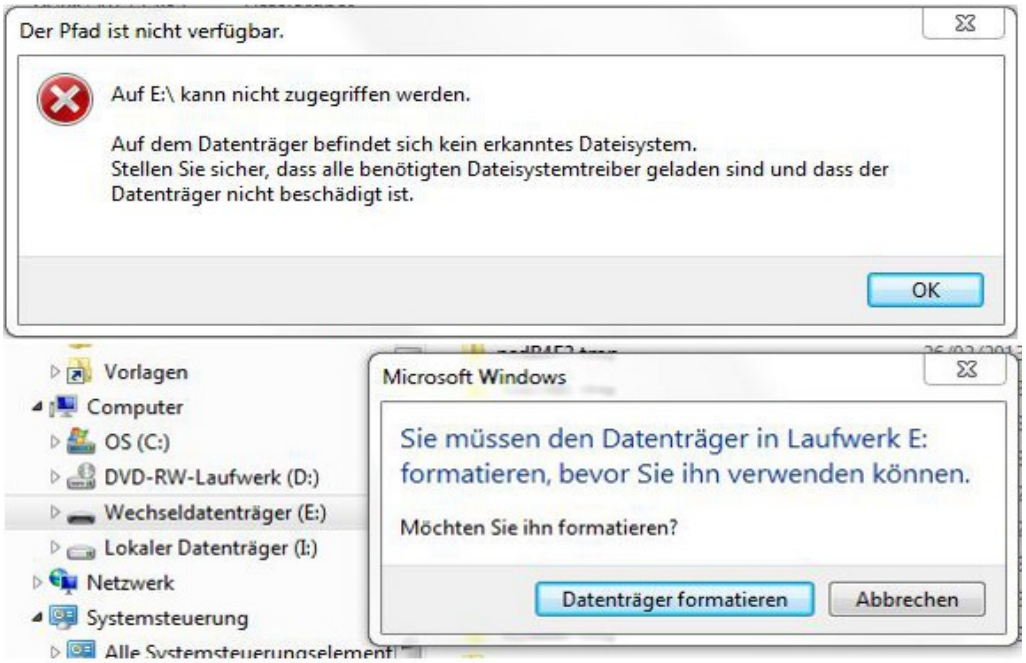
Caschys Blog: Mit TrueCrypt unterwegs
http://stadt-bremerhaven.de/mit-true-crypt-unterwegs/

Caschys Blog: Dropbox und TrueCrypt – verschlüsselte Daten in der Cloud (Windows und Mac)
http://stadt-bremerhaven.de/dropbox-und-truecrypt-verschluesselte-daten-in-der-cloud/

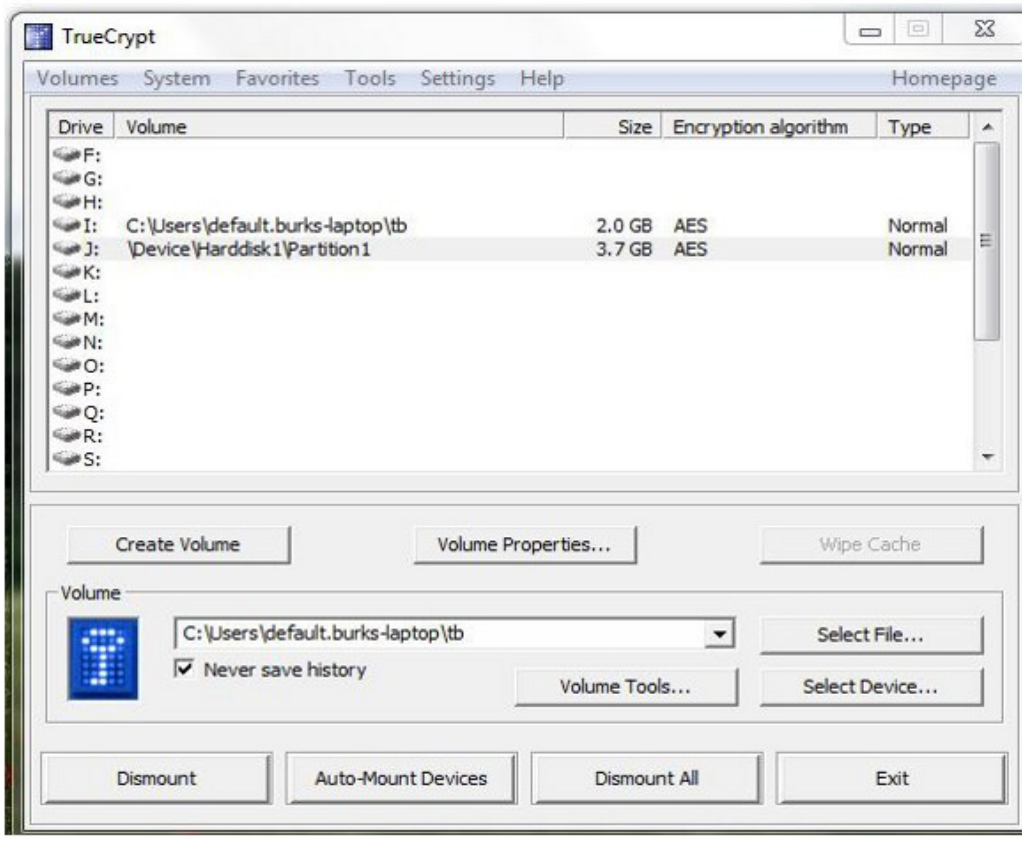
Caschys Blog: TrueCrypt Container unter Mac OS X automatisch mounten (nicht ganz einfach)
http://stadt-bremerhaven.de/truecrypt-container-unter-mac-os-x-automatisch-mounten/

3. Schritt

"Hidden Container" eignen sich gut für USB-Sticks. Diese werden nur sichtbar, wenn Sie "Auto-Mount Devices" wählen. Das Feature “Hidden Container” könnte wichtig werden, wenn Sie bei der Einreise in ein anderes Land gezwungen werden sollten, Ihr Laptop zu öffnen oder gar Ihre Truecrypt-Container.



Auto-Mount Devices:



Argumente gegen “Anti-Viren-Programme”

Erstes Argument: Ein Windows-Nutzer (Version Vista ff) wird penetrant dazu aufgefordert, den so genannten "Defender" zu aktivieren – "eine Sicherheitssoftware der Firma Microsoft zur Erkennung von potenziell unerwünschter Software (vorwiegend Spyware)".

Wenn diese "Sicherheitssoftware" etwas nützten, warum sollte man noch zusätzliche "Antivirenprogramme" installieren? Was ist denn eigentlich das Geschäftsmodell der Hersteller wie Kaspersky oder McAfee, da Windows Defender doch behauptet, es schütze die Rechner gegen schädliche Software? Und was ist das Motiv der Leute, die deren "Sicherheitssoftware" benutzen? "Doppelt hält besser", "einem geschenkten Gaul schaut man nicht ins Maul" oder "man kann nie wissen"?

Zweites Argument: Antivirenprogramme tun nicht das, was sie behaupten, und sie wirken nicht hinreichend. Um das zu belegen, muss man nur den einschlägigen Wikipedia-Eintrag lesen:

Virenscanner können prinzipiell nur bekannte Schadprogramme (Viren, Würmer, Trojaner etc.) bzw. Schadlogiken (engl. Evil Intelligence) erkennen und somit nicht vor allen Viren und Würmern schützen. Daher können Virenscanner generell nur als Ergänzung zu allgemeinen Vorsichtsmaßnahmen betrachtet werden, die Vorsicht und aufmerksames Handeln bei der Internetnutzung nicht entbehrlich macht. So fand die Stiftung Warentest bei einem "internationalen Gemeinschaftstest" von 18 Antivirusprogrammen Anfang 2012 mit 1.800 eingesetzten "aktuellen" Schädlingen Werte von 36 bis 96 % aufgespürten Signaturen.

Das Ergebnis der Stiftung Warentest ist übrigens transparent und für die Lobby der Antivirensoftware-Hersteller vernichtend.

Drittes Argument: Die Hersteller der Antivirenprogramme spähen selbst die Rechner der Nutzer aus und erhalten sensible Informationen nicht nur über alle installieren Programme. Man sollte zum Beispiel die "Lizenzbedingungen" Kasperkys studieren.

Viertes Argument: Die so genannte "Sicherheitssoftware" oder die Antivirenprogramme sind oft selbst schädlich oder versagen kläglich, wenn es darauf ankommt. Beispiele: "Windows Defender ermöglicht Einbruch in Windows-Systeme" (Heise, 05.04.2013). "Antiviren-Software AVG hielt Systemdatei für Trojaner" (Heise, 14.03.2013). "Why Antivirus Companies Like Mine Failed to Catch Flame and Stuxnet" (Wired, 06.01.2012). "Apple lehnt Antivirensoftware von Kaspersky für iOS ab" (TNW, 05.02.2013).

Fünftes Argument: Die Lobby der Antivirenprogramm-Hersteller versucht, ihre Produkte heimlich und auf Umwegen auf den Rechnern unerfahrener Nutzer zu installieren, zum Beispiel über Updates anderer Programme. IT-Portale warnen ausdrücklich davor. (Heise, 27.02.2013) Das ist definitiv kein seriöses Geschäftsgebaren.

Sechstes Argument: Unerfahrene Nutzer, die sich durch die Propaganda der Lobby für Antivirenprogramme einschüchtern lassen oder auf die dämliche und unkritische Berichterstattung der Mainstream-Medien hereinfallen, werden mit den Ergebnissen der "Prüfung" ohnehin wenig anfangen können."

Siebtes Argument: Wer sich vernünftig verhält, braucht keine zusätzliche Software, um irgendetwas abzusichern.

Links

Datensicherheit

Truecrpyt (für alle Betriebssysteme, kostenlos)
http://www.truecrypt.org
Deutsches Sprachpaket:
http://www.truecrypt.org/localizations

Cloud
https://de.wikipedia.org/wiki/Cloud-Computing
Nur homomorphe Verschlüsselung ist sicher (der Anbieter bekommt keine Klartext-Dateien zu sehen). Das kann aber auch gelöst werden, indem der Kunde die auf seinem eigenen Rechner verschlüsselten Daten (mit Truecrypt oder PGP/OpenPGP) in der Cloud speichert.
https://de.wikipedia.org/wiki/Kryptographie#Homomorphe_Verschl.C3.BCsselung

Anbieter (auch für Smartphones) z.B. Wuala
http://www.wuala.com/
http://www.wuala.com/en/support/faq/c/20

Smartphone:
Browser (vgl. Modul 2)
Orbot: Proxy with Tor (Tor-Proxy)
https://play.google.com/store/apps/details?id=org.torproject.android&hl=en
zusammen mit Orweb (Browser für anonymes Surfen)
https://play.google.com/store/apps/details?id=info.guardianproject.browser&hl=en

E-Mail-Verschlüsseln (optional, bis jetzt keine benutzerfreundliche App verfügbar)
APG
https://play.google.com/store/apps/details?id=org.thialfihar.android.apg

EDS (alternative für Truecrypt auf Smartphones)
https://play.google.com/store/apps/details?id=com.sovworks.eds.android&hl=en

App-Kontrolle: Permissions Observatory
https://play.google.com/store/apps/details?id=org.quet.android.po&hl=en

Überwachung und Datenspionage:

PRISM (Überwachungsprogramm)
http://de.wikipedia.org/wiki/PRISM_%28%C3%9Cberwachungsprogramm%29

Tempora
http://de.wikipedia.org/wiki/Tempora

Zeit online(21.03.2013:
Bundestag erlaubt Polizei Abfrage von PIN und Passwörtern
http://www.zeit.de/digital/datenschutz/2013-03/bestandsdaten-breyer-bundestag

Süddeutsche Zeitung (24.06.2013): Briten schöpfen deutsches Internet ab - Der Londoner Geheimdienst GCHQ hat nach Recherchen der SZ und des NDR in großem Umfang deutsche Übersee-Kommunikation über Telefon und E-Mail abgeschöpft.
http://www.sueddeutsche.de/politik/nachrichtendienst-gchq-briten-schoepfen-deutsches-internet-ab-1.1704670