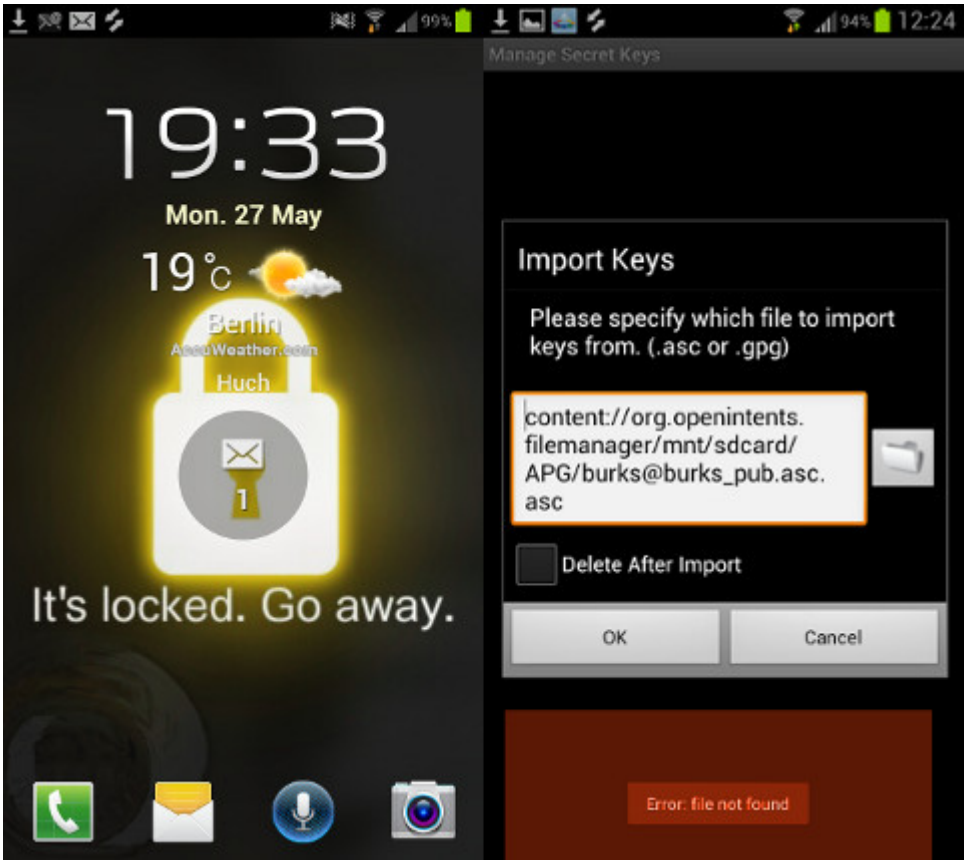
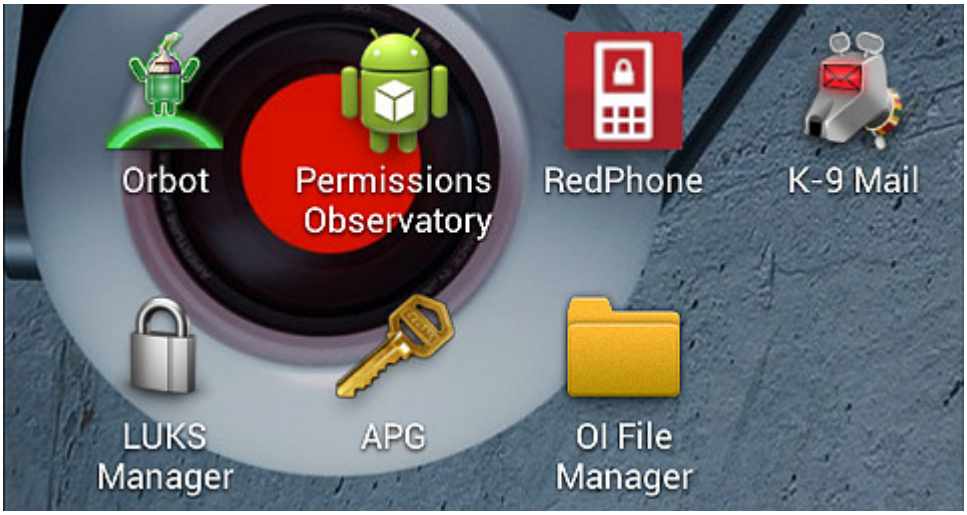
APG: can’t import private or public key on internal sd card [Update 2]



Ich rüste gerade mein Smartphone auf, so dass die Sicherheitsstandards so sind wie auf meinen anderen Rechnern. Das heißt: E-Mail-Verschlüsselung, Hochsicherheits-Browser, anonymes Surfen als Option möglich, relevante Daten nur in verschlüsselten Containern (Truecrypt gibt es noch nicht für Android, deshalb ist die App LUKS Manager zu empfehlen – ich arbeite daran, das volkstümlich darzustellen.)



Ich habe aber ein Problem, bei dem ich nicht weiterkomme. Als E-Mail-Programm auf dem Smartphone empfehle ich K-9 Mail; das ist um Längen besser als die Standard-E-Mail-Application, die bei mir alle fünf Minuten einfriert und abraucht und deshalb untauglich ist.

Um E-Mails auch auf dem Smartphone zu verschlüsseln, braucht man die App APG (Android Privacy Guard).

Ich habe dem Entwickler geschrieben, aber der antwortet nicht:

I have the same problem as it has been described here already, but I can’t fix it:
code.google.com/p/android-privacy-guard/issues/detail?id=103
code.google.com/p/android-privacy-guard/issues/detail?id=59
I cannot export or import any key/file.
I am using Samsung Galaxy S3 with K 9 mail and APG.
I tried to type the file name too, but I can’t even export my new created public and secret keys.

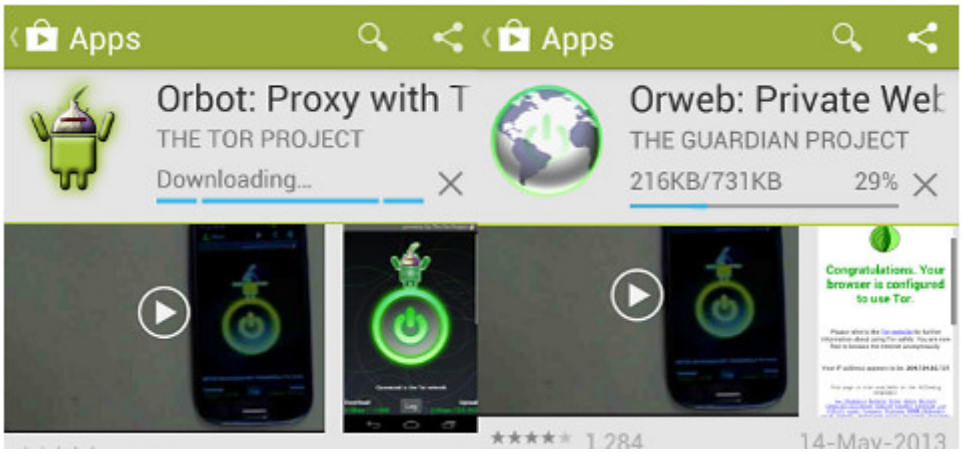
I imported my keys from my computers (renamed the keys before), any filemanager as OI File manager shows them, but nothing works (Error: file not found)

Hat jemand einen Tipp, woran das liegen könnte?

[Update] Ich lese gerade Die Androiden-Toolbox, vieleicht wird mir das weiterhelfen.

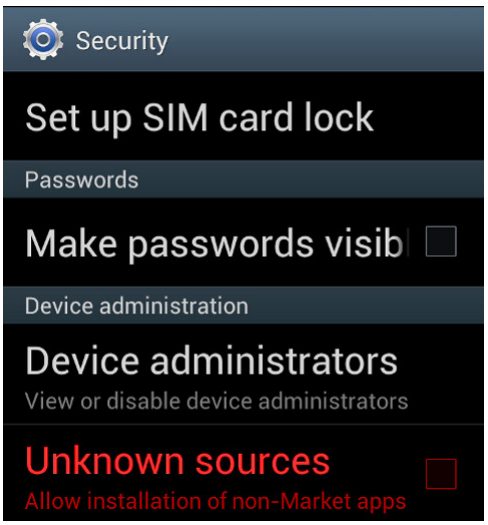
[Update 2] Es hat irgendetwas mit dem Dateimanager zu tun. Mir gelingt es zur Zeit auch nicht, die Database files von KeePassDroid einzubinden, obwohl die unstrittig schon auf dem Smartphone sind…

Anonym Surfen mit dem Smartphone



Oder auch: Secure Mobile Apps and Open-Source Code for a Better Tomorrow – sichere mobile Anwendungen und Open-Source-Software für eine bessere Zukunft.

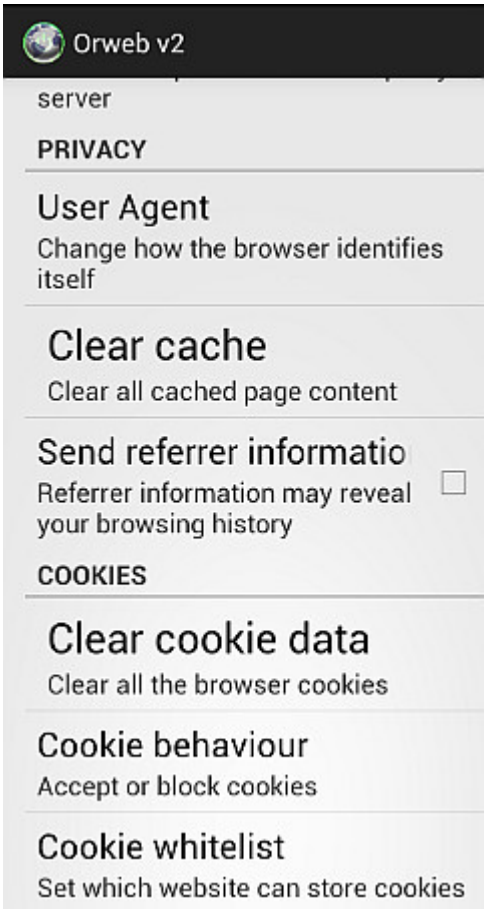
Eine der Geschäftsideen der Anbieter von Smartphones fußt auf der Datenspionage und dem Verkauf des Nutzerverhaltens. Das funktioniert hervorragend, werden doch die gewöhnlichen DAUs von faulen und unfähigen „Webdesignern“,



von Microsoft und Apple und von „Computerexperten“, die in den Mainstream-Medien zu Wort kommen, zu unsicherem Surfen ermutigt, erzogen, ja teilweise gezwungen.

Man sollte diesen Leuten aber eine Menge Sand in ihr gieriges Datenkrakengetriebe werfen. Für Smartphones gibt es zwei nette Anwendungen („Apps“), mit denen man anonym surfen kann: Orweb und Orbot (Proxy mit Tor). Orbot ist ein Proxy („Vermittler„), der die Daten zwischem dem Browser Orweb und dem Tor-Netz transportiert und Anonymität garantiert.

Man kann per Google Store die beiden Apps auf das Smartphone laden oder zunächst auf einen Rechner und von dort dann auf das gar nicht so „smarte“ Handy. Vernünftige Menschen schauen zunächst in die Voreinstellungen eines unsicheren Gerätes, bevor sie es in Betrieb nehmen: Normalerweise sollte man *verbieten*, dass Apps aus unbekannten Quellen installiert werden dürfen (also *kein* Häkchen). Hier müssen wir es ausnahmsweise erlauben (vgl. 2. Screenshot von oben).



Das *Guardian Project* sagt klar und angenehm, was erstens zweitens drittens käm:

Orweb is the most private and anonymous web browser on Android for visiting any website, even if it's normally censored, monitored, or on the hidden web.

– ACCEPT NO SUBSTITUTES: Orweb is the safest browser on Android. Period. Orweb evades tracking and censorship by bouncing your encrypted traffic several times through computers around the world, instead of connecting you directly like VPNs and proxies. This process takes a little longer, but the strongest privacy and identity protection available is worth the wait.

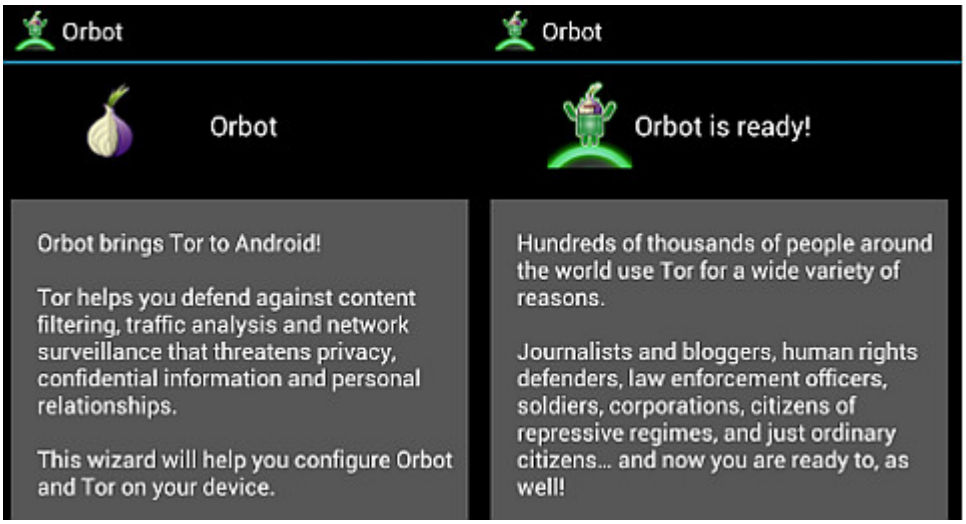
– CIRCUMVENT FIREWALLS AND RESTRICTIONS: Does your office, school, or region block certain websites? Not anymore. Orweb bypasses almost every kind of network restriction.

– BROWSE ANONYMOUSLY: As the New York Times writes, "when a

communication arrives from Tor, you can never know where or whom it’s from.” No technology is 100% effective, but Orweb is as close to anonymous as it’s possible to get on Android.

– PRIVACY YOU CAN TRUST: The Electronic Frontier Foundation (EFF) says „the groundbreaking work from the Tor project helps users everywhere improve the safety of their online communications.“

Fazit auf Deutsch: Orweb ist der sicherste Browser auf Android. Akzeptiere nie Zensur oder (Jugendschutz-)Filter, sondern umgehe sie. Orweb bietet die größtmögliche Anonymität. Die EFF sagt, das Tor-Projekt helfe allen Usern weltweit, sicher zu kommunizieren. Die EFF ist so etwas wie der Chaos Computer Club, nur ohne Verschwörungstheoretiker und Mobbing von Kritikern, dafür aber wesentlich politischer und libertärer.

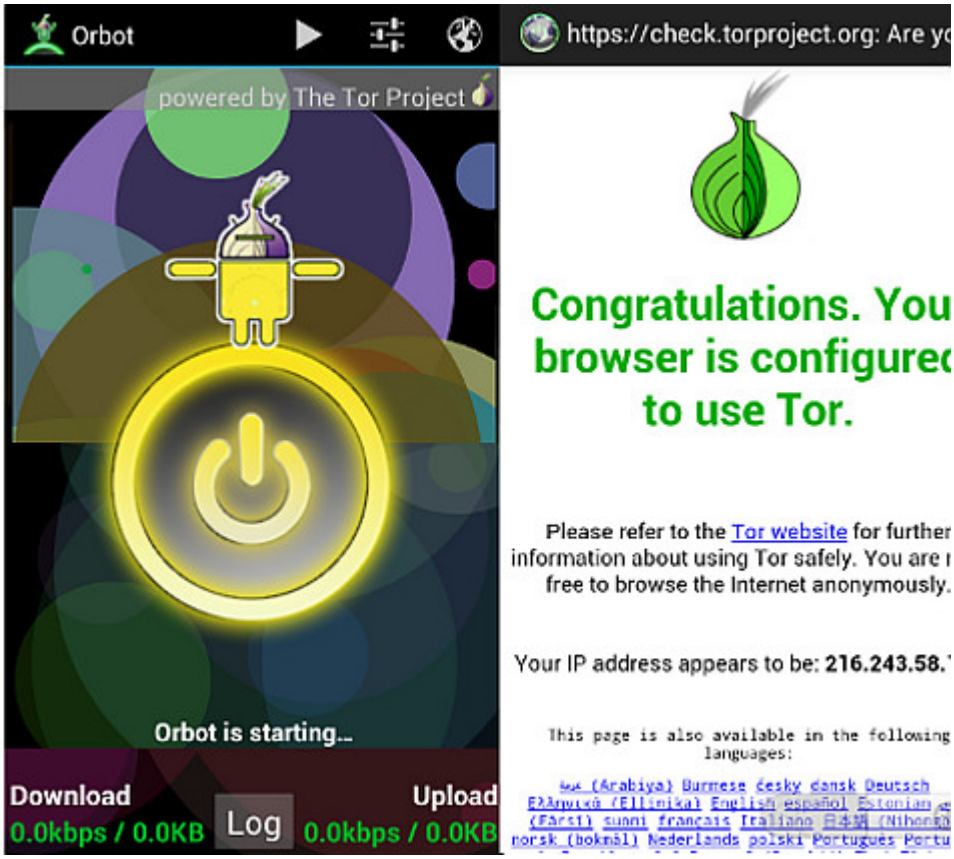


Wenn beide Apps installiert worden sind (nicht vergessen: das Häkchen in den „Options“ wieder entfernen, dass unbekannte Quellen installiert werden dürfen!), muss man sich – wie bei anderen Rechnern – mit den Voreinstellungen des Browsers beschäftigen. Wer Cookies, Referer und Javascript erlaubt, kann auch gleich das Schloss vor die Haustür nageln. (vgl. 3. Screenshot von oben)

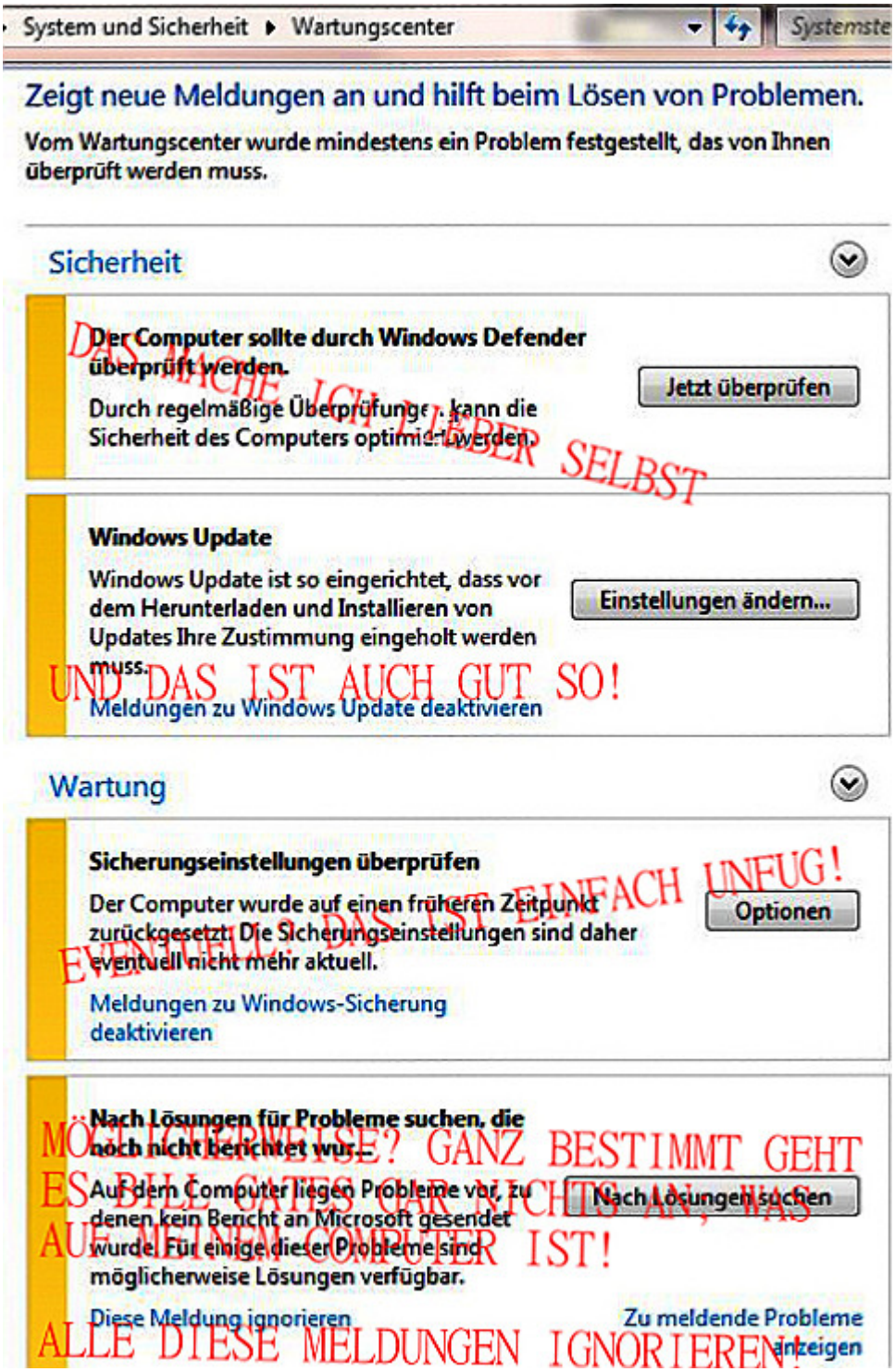
Im Unterschied zum Tor Browser Bundle, der ohne weitere

Zusätze das anonyme Surfen ermöglicht, braucht *Orweb* den Proxy *Orbot*, den man zuerst einschalten muss. Bei mir hat die ganze Angelegenheit – Installieren und Einrichten – zehn Minuten benötigt.

Die Browser-Nutzeroberfläche verwirrt, weil man den „Go“-Button, der die Eingabe des Urls ermöglicht, nicht sofort findet (weil man danach nicht sucht). Ansonsten ist das Surfen wie gewohnt. Man hinterlässt nur keine Datenspuren mehr.

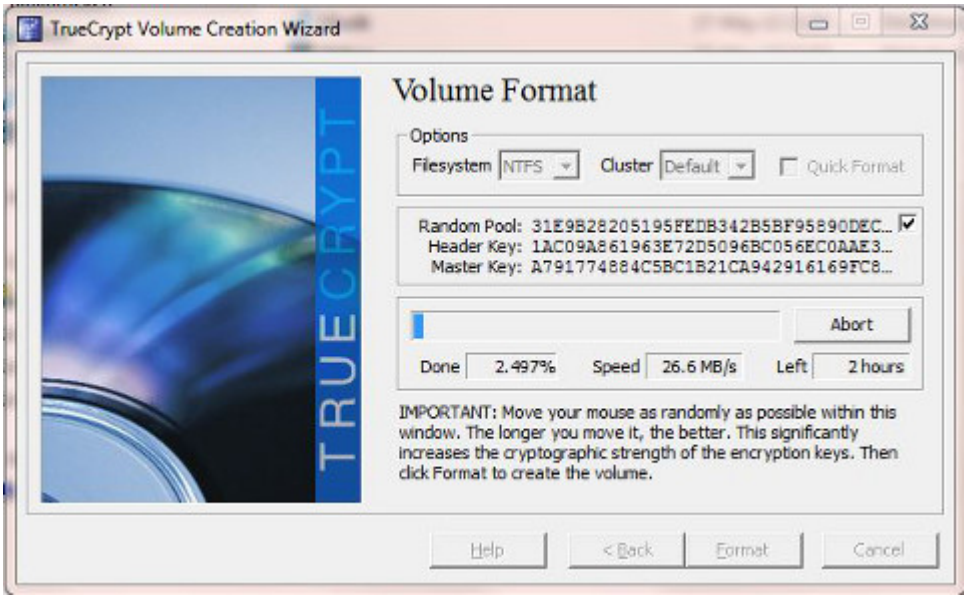


Alles Ignorieren



SOKO Vorabendserie: Auf dem

Computer des Verdächtigen haben wir gefunden



Leider kenne ich keinen Professor, der an irgendeiner Film- oder Fernseh~~akademie~~ sonstigen ~~Hoch~~Schule lehrt, wie man Drehbücher schreibt. Dem oder der würde ich gern einmal ein Forschungsprojekt vorschlagen, das auch gern in einem Buch enden könnte, mit dem Arbeitstitel: „Computer-Voodoo in deutschen Kriminalfilmen“. Es ist oft zum Haareraufen, was dort gezeigt und behauptet wird, wenn es um Internet und Rechner geht. Ein Regen- oder Schamanen-Tanz auf Samoa ist gar nichts dagegen.

Sogar das Raten des Passworts kommt immer wieder vor. Fällt denen eigentlich nichts Realistisches ein? Liebe Drehbuch-VerfasserInnen: Man kann Computer und Daten so absichern, dass niemand (in Worten: überhaupt keiner) mehr etwas finden kann, auch nicht die ~~KTU~~ „EDV-Abteilung“ im Keller einer Fernseh-SOKO.

Sätze wie „Auf dem Computer des Verdächtigen haben wir dieses oder jenes gefunden“ (gestern wieder: SOKO Wien) sind einfach totaler Quatsch und primitive Magie.

Einschränkend muss man natürlich zugeben, dass die breite ~~Ich glotz TV~~ gehirnweiche Masse sich genau so bescheuert verhält, was Internet, Computer und Sicherheit angeht, wie diejenigen, die dazu passende Drehbücher schreiben.

Es ist ein geschlossenes System, wie auch schon beim Medien-Hype um die so genannte „Online-Durchsuchung“: Die Mainstream-Medien oder irgendjemand, dem die Medien aus unbekannten Gründen zuhören (jemand, der im Notizbuch eines Journalisten steht, weil er bei einem bestimmten Thema immer vor jedes Mikrofon springt) behaupten etwas, was dann in der Populärkultur und in der *daily soap* solange ins Bewusstsein eingehämmert wird, bis es jeder glaubt (wie schon beim Diskurs über „Rauschgift“) – und das dann wiederum von den Medien als „Wahrheit“ zitiert wird.

Wer sich dagegen stemmt, gerät schnell in die Rolle des Kindes, das ruft: „Aber der Kaiser ist doch nackt“. Dieses Märchen sagt mehr über die Mechanismen unserer Gesellschaft aus – Opportunismus, Feigheit, Dummheit, Trägheit der Masse – als 100 Philosophie- und Soziologie-Bücher zusammen.

Wir schweifen ab. Ich wollte sagen: Auch externe und Backup-Medien sollten komplett mit Truecrypt verschlüsselt werden. („Encrypts an entire partition or storage device such as USB flash drive or hard drive.“)

Skype: You are not the customer – you are the

product being sold!

Skype war schon immer eine Malware und en Einfallstor für andere Spionage-Programme, die im DAU-Volksmund als „(Bundes-)Trojaner bezeichnet werden.

Ich hatte 2008 in der Netzeitung Alternativen vorgestellt und hier (09.10.2012) über die Programme gebloggt, die die gern zitierten „Sicherheitskreise“ nutzen, um mitzuhören. (Vgl. Mega – panzer.com, 25.08.2009: „Skype trojan sourcecode available for download“).

Heise hat jetzt bestätigt, dass auch Microsoft – der neue Eigentümer – Gespräche mitliest. Zitat zum Mitschreiben: „wer Skype benutzt hat echt keine Ahnung von IT“.

Im Heise-Form las ich übrigens auch den interessanten Hinweis auf ejabberd.

Ich frage mich aber, ob das Abhören die originäre Skype-Software benötigt oder ob nur der Datenstrom gesnifft wird. Ich habe auch einen Skype-Account, nutze den aber, wenn ich in die USA telefoniere, nur mit Trillian. Da ich auf dem Balkon sitze und den lauen Abend genieße, bin ich zu faul, das zu recherchieren. Wozu gibt es die wohlwollenden Leserinnen und geneigten Leser…

Sieben starke Argumente gegen Antivirenprogramme

Gestern diskutierte ich mit einem Freund, der über Computer et al mehr weiß als ich, kontrovers über den Einsatz von Antivirenprogrammen und ob man Windows-Nutzern (Linux-Nutzer brauchen das eh nicht) empfehlen sollte, so etwas anzuschaffen oder nicht. Ich sagte nein, er sagte, ich sei so arrogant wie Fefe und man müsse gewöhnlichen DAUs doch raten, Kasperskymcaffeeoderwiesielleheissen zu installieren.

Da ich während des Gesprächs nicht mehr ganz nüchtern war und auch die gegenwärtige Dame meines Herzens neben mir saß und mich temporär ablenkte, musste ich das Für und Wider heute noch einmal erwägen und in meinem steinern-sturen Herzen hin- und herwenden. Nein, ich bleibe bei meiner Meinung. Weg mit dem ~~Schlangenöl~~ Zeug!

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)“.

Ach?! Wenn diese „Sicherheitssoftware“ etwas nützte, warum sollte man denn 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 ~~Schlangenöl-Hersteller~~ Antivirensoftware-Hersteller vernichtend. Kein Wunder, dass denen das nicht gefällt.

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 (ich lese immer das Kleingedruckte). Da weiß man, was man bekommen hat. Zum Gruseln.

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“ (