Geheime gefährliche Listen

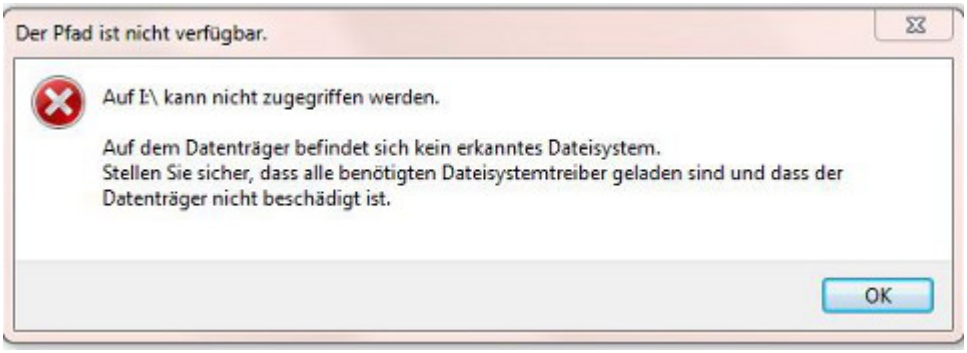
Die geheime (!) Liste der BPjM von angeblich „jugendgefährdenden Medien“, die geleakt wurde, findet man auf Twitter unter #bpjmleak.

Junk

Daily Mail: Angelina Jolie hat früher ein Handy mit Antenne benutzt. SCNR. Wer sich für Fußball interessiert, ist auch hier gut bedient.

BTY liebe Netzgemeinde, was die Menschen wirklich interessiert, ist das:
The match became Twitter’s most discussed sports game ever, with 35.6 million tweets sent by users. It easily beat the previous record of 24.9 million tweets set by the Super Bowl earlier in 2014. The game also broke the record for the most tweets per minute – when Germany’s Sami Khedira’s scored the team’s fifth goal in the 29th minute Twitter saw 580,166 tweets per minute.

Wetter-Apps und Kryptoprogramme



„Bei einer Wohnungsdurchsuchung stießen die Ermittler auf einen Computer, dessen Sofware-Konfiguration so aussieht, als ob sie ein Geheimdienst präpariert habe. Auf dem Rechner ist eine Wetter-App installiert, fragt der Nutzer das Wetter in New York ab, öffnet sich automatisch ein Kryptoprogramm.“ (Aus dem aktuellen Spiegel über den enttarnten BND-Agenten)

Super. Jetzt weiß ich endlich, wie ich meine Rechner konfigurieren muss. Ich würde aber das Wetter in Tel Aviv oder auf der Krim abfragen. Die Links auf die Truecrpyt-Container auf dem Desktip Windows-Rechner sind öffenbar nicht intelligence-kompatibel, obwohl sich beim Klicken darauf ein „Kryptoprogramm“ öffnet. Da das ehemalige Nachrichtenmagazin uns nicht verrät, um welches „Kryptoprogramm“ es sich handelt, obwohl uns das am meisten interessiert, kann man nur vermuten, dass ~~der Volontär~~ die fünf Redakteure, ~~der~~ die von der Agitprop-Abteilung des Verfassungsschutzes gebrieft wurde, diesen Artikel zu ~~lancieren~~ schreiben, nicht interessiert waren genau zu wissen, was in Wahrheit geschehen ist.

Welt online formuliert vorsichtig: „Noch größer ist die Verwunderung darüber, dass der Verdächtige sich am 28. Mai dieses Jahres unter Beifügung vertraulicher Dokumente von einem Google-Mail-Account aus an das russische Generalkonsulat in München gewandt hatte.“ Sicher, und auch noch unverschlüsselt.

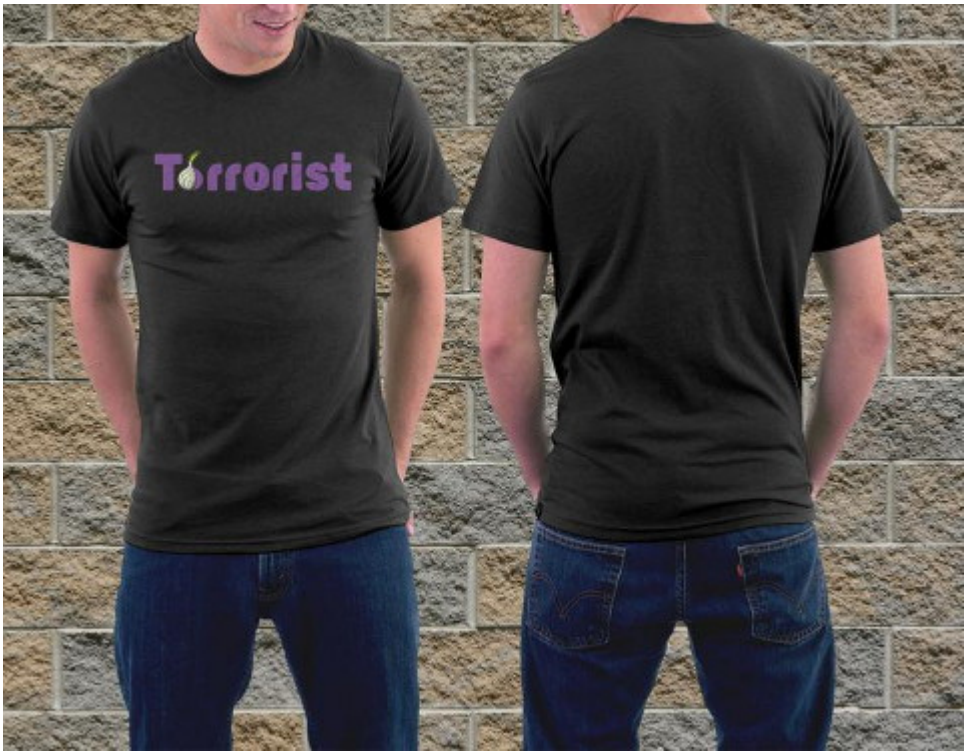
Faszinierend, wie kompetent die BND-Mitarbeiter im Dienste der USA sind, die den NSU-Untersuchungsausschuss ausschnüffeln sollten. „Tatsächlich las der Verfassungsschutz die Mail an

das russische Konsulat mit.“ Ach?! Der Verfassungsschutz hat jetzt vielleicht auch V-Leute beim BND. Har har.

„Stefan Wels vom NDR sagte in der Tagesschau, die Ermittler hätten das Haus der Verdächtigen durchsucht und dabei einen USB-Stick sichergestellt. Dieser werde ausgewertet“, meldet die Tagesschau. Und ganz bestimmt hat die BND-Pappnase auf seinem USB-Stick kein *hidden volume*. Das wäre nicht kompatibel mit Wetter-Apps und auch zu kompliziert, dass Verfassungsschützer und Journalisten das verstehen würden.

Wisst ihr was? Ich glaube dieser Sau, die gerade ~~durch die Netzgemeinde~~ durchs Dorf getrieben wird, kein Wort. Ein Geheimdienst, der „Kryptoprogramme“ hinter Wetter-Apps versteckt, ist eine Lachnummer. Für mich sieht das wie eine – gewohnt dilettantisch gemachte – Nebelkerze des Verfassungsschutzes aus, der genau weiß, dass diejenigen Journalisten, die zu solchen Briefings eingeladen werden, nicht nachhaken, sondern alles brav mitschreiben und genau so publizieren. Just my 20 Cents.

Unter Torroristen



Aus der Tor-Mailingliste:

I would like to quote from the XKeyscore code (1)(2):

> *„// START_DEFINITION*
> */**
> *These variables define terms and websites relating to the TAILs (The Amnesic Incognito Live System) software program, a comsec mechanism advocated by extremists on extremist forums.*
> **/*
>
> *$TAILS_terms=word(‚tails‘ or ‚Amnesiac Incognito Live System‘) and word(‚linux‘ or , USB , or , CD , or ’secure desktop‘ or , IRC , or ‚truecrypt‘ or , tor ,);*
> *$TAILS_websites=(‚tails.boum.org/‘) or (‚linuxjournal.com/content/linux*‘);*
> *// END_DEFINITION“*

Obviously we on these lists belong to the most extreme dangerous people one can think of :-)) . Pirate Party Luxemburg thinks the same and offers for 20 EUR or 0.043 BTC a nice TORrorist Shirt (3). The profit will be donated to the

Tor project.

Best regards and stay wiretapped!

Bange machen gilt nicht

Ein Kommentar von mir in der taz: „Wer hat Angst vor der bösen NSA? – Ja, ich bin ein Extremist – im Sinne der NSA. Ja, ich bekenne: Ich habe Tor und andere Anonymisierungsdienste genutzt und werde das weiterhin tun. Ich beschäftige mich oft mit dem Thema und suche im Internet danach. Deswegen bin ich in der NSA-Datenbank XKeyscore vermutlich schon gespeichert. Wenn nicht, wäre ich empört. Ich hielte es für unerträglich, wenn das Imperium des Bösen mich für harmlos hielte. [mehr…]

Sensationell ist, dass die taz mehr Links in den Artikel hineingedröselt hat als ich in das Original-Manuskript… Geht also.

In der Mitte meines Manuskripts hieß es: „Viel schlimmer als diejenigen, die keine Ahnung von Sicherheit im Internet haben wollen, sind die Defätisten, die mit geheimnisvoller Miene murmeln: „Die sind eh schon drin. Man kann nichts tun.“ Hier meine Verschwörungstheorie: Vermutlich werden gerade die von Geheimdiensten bezahlt. Das genau wollen die erreichen: Dass niemand mehr etwas unternimmt.“

Der letzte Satz sollte heißen: „Wer nach einer Reform oder gar einer Kontrolle der Dienste ruft, ist nicht nur naiv, sondern vergisst – oder ist nur zu feige – die Systemfrage zu stellen.“ (hat die taz mittlerweilie ergänzt).

Techniken der Datensammler: Was dagegen tun?

Jondonym stellt die Techniken der Datensammler vor, fasst die Risiken zusammen und gibt gleichzeitig Argumentationshilfen, warum man sicher und anonym surfen sollte:

– Tracking mit Cookies: Cookies sollte man ganz ausstellen!

– Flash-Cookies und EverCookies: Dagegen hilft z.B. das Firefox-Add-on Better Privacy.

– Fingerabdruck des Browsers: „Das Demonstrations-Projekt Panopticlick der EFF zeigt, dass mehr als 80% der Surfer anhand des Fingerabdrucks des Browsers eindeutig erkennbar sind. (…) Es werden die verwendete Software (Browser, Betriebssystem), installierte Schriftarten, Bildschirmgröße und Browser-Plugins ausgewertet. Zusätzliche Informationen werden mit einem Flash-Applet gesammelt. Bluecava erreicht damit bis zu 30% bessere Erkennungsraten, als Cookie-basierte Lösungen."

– Cache des Browsers: Cache beim Herunterfahren des Browsers löschen – das kann man so einstellen.

– Referer: Abhilfe z.B.: RefControl.

– Risiko JavaScript (ausschalten! Empfehlenswert: Noscript: „Das FBI nutzte im August 2013 bösartige Javascripte, die auf Tor Hidden Services platziert wurden, um durch Ausnutzung eines Bug im Firefox einen Trojaner zu installieren und Nutzer des Anonymisierungsdienstes zu deanonymiseren." (Sorry, aber wer Tor nutzt und gleichzeitig Javascript erlaubt, sollte geteert und gefedert werden – mein Mitleid hält sich da in

Grenzen.)

– Risiko Plug-ins: „Der (Staats-) Trojaner der Firma HackingTeam wird beispielsweise mit einer signierten JAR-Datei auf dem Zielsystem installiert. Der Trojaner belauscht Skype, fängt Tastatureingaben ab, kann die Webcam zur Raumüberwachung aktivieren und den Standort des Nutzers ermitteln. Nur das Deaktivieren aller Plug-ins im Browser bringt Sicherheit.“ Java deaktivieren! Statt Adobe kann man auch den Foxit-Reader neben. Ich habe Adobe-Produkte übrigens komplett von meinen Rechnern entfernt.

– History-Sniffing: Abhilfe: keine History bzw. Browserverlauf anlegen.

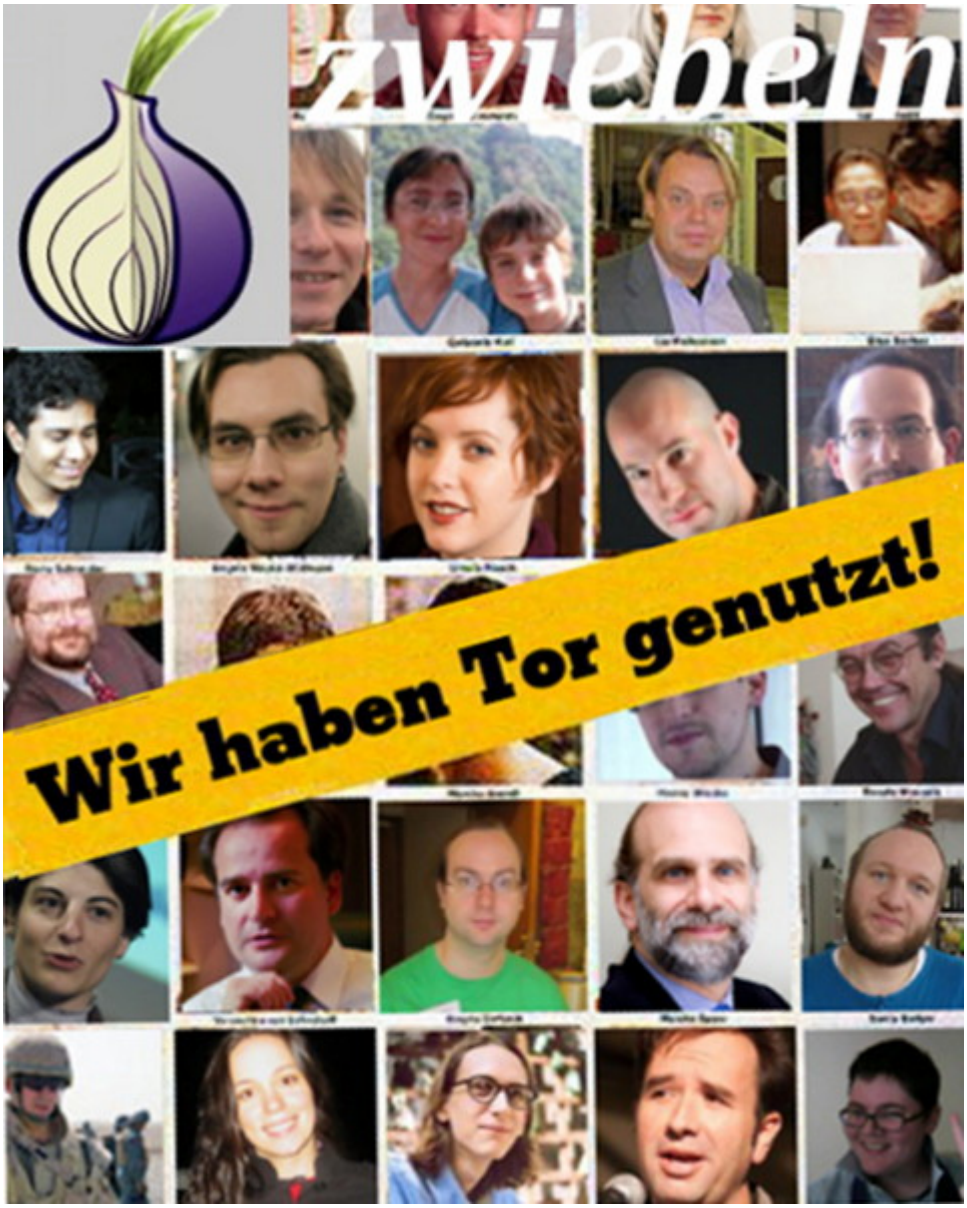
– Webbugs, Werbebanner und Like-Buttons: „Eine andere unangenehme Eigenschaft von Webbugs ist, dass sie beim Abruf neben Cookies auch Ihre IP-Adresse automatisch an den Statistikdienst übermitteln. Selbst mit einer sehr guten Browserkonfiguration, dem Abschalten von Cookies und automatischen Webbug-Filtern können Sie dies niemals zuverlässig verhindern. Dagegen hilft nur die Verwendung eines Anonymisierungsdienstes.“

– TCP-Zeitstempel: Der Zeitstempel kann vom Client- und/oder Server-Gerät eingesetzt werden, um die Performance zu optimieren. „Jedoch kann ein Internetserver Ihren Computer anhand der Zeitstempel wiedererkennen und verfolgen: Indem er die Abweichungen in der Uhrzeit misst, kann er ein individuelles Zeit-Versatz-Profil für Ihren Computer berechnen. Außerdem kann er die Zeit schätzen, zu der Ihr Rechner zuletzt neu gestartet wurde.“ Abhilfe nur per Anonymisierungsdienst.

– IP-Adresse: Die IP-Adresse offenbart zum Beispiel den aktuellen Aufenthaltsort, den Zugangsprovider, die Anbindung und Zugangstechnologie, das Unternehmen / die Behörde. Abhilfe nur per Anonymisierungsdienst.

– MAC-Adresse (kann man selbst ändern!).

Ich bekenne: Auch ich bin ein Extremist



Völkerkunde 2.0 oder: Weak Ties

Technology Review:
Wäre Facebook ein Land, seine 900 Millionen Nutzer würden die drittgrößte Nation der Erde stellen. (…) In einer Hinsicht jedoch stellt „Facebook-Land“ jeden anderen Staat in den Schatten: Mit dem, was es über seine Bewohner weiß. Facebook zeichnet sämtliche digitalen Bewegungen seiner virtuellen Bürger auf. Selbst die großen Despotien der Vergangenheit wirken blass angesichts des Ausmaßes, in dem Facebook Gespräche, Familienfotos, Aufenthaltsorte, Beziehungsverhältnisse, Freundschaften und sogar Todesfälle speichert.

Money quotes: „‚Wir haben zum ersten Mal ein Mikroskop, mit dem wir menschliches Verhalten nicht nur sehr feinkörnig auflösen können, genauer als je zuvor, sondern mit dem wir auch Experimente machen können – Experimente mit Millionen von Nutzern‘, sagt Marlow.“

„Dabei fand er heraus, dass unsere engsten Freunde zwar einen starken Einfluss darauf haben, was wir teilen. Doch ist dieser Effekt noch gering im Vergleich zum kollektiven Einfluss der zahlreichen Bekannten im Netzwerk. Soziologen nennen solche Bekanntschaftsbeziehungen „weak ties“, schwache Bindungen“.

„Denn wer die Mechanik der sozialen Beeinflussung versteht, kann Online-Werbung noch eindrücklicher gestalten und damit bewirken, dass die Nutzer noch häufiger auf Anzeigen klicken.“

Da ich kaum *weak ties* habe, bin ich vermutlich auch schwer zu beeinflussen. Burks gefällt das.

Wir sind nicht allein!

„Wer seinen Rechner einschaltet, muss sich bewusst sein, dass er von dem Moment an nicht mehr allein ist. Egal, wer sich da gerade reinhackt, ob das die Chinesen oder die Amerikaner oder die Russen sind. Es ist doch nichts Neues, dass all diese Länder Daten einsammeln.“ (Lorenz Caffier, Innenminister Mecklenburg-Vorpommern in Zeit online, via Hal).

Der Herr Forstfacharbeiter („Ich bin das, was man nach der Wiedervereinigung eine Blockflöte genannt hat“) ist offenbar auch eine Pfeife. Wer sich wohl in dessen Kopf gehackt hat?

NSA backdoors per default

Electronic Frontier Foundation (EFF): „Today, the US House of Representatives passed an amendment to the Defense Appropriations bill designed to cut funding for NSA backdoors.“

Vgl. auch Heise: „US-Repräsentantenhaus votiert gegen NSA-gesponserte Sicherheitslücken.“

Die Pointe an der Sache ist, dass der Foreign Intelligence Surveillance Act (Sektion 702), also das Gesetz (eines von mehreren), welches das Abhören regelt, nur Personen zu überwachen erlaubt, „die mit 51-prozentiger Sicherheit keine US-Amerikaner sind.“ Ab Werk eingebaute Sicherheitslücken und Schnittstellen zum Überwachen würden aber auch US-Amerikaner treffen. Heise: „Darüber hinaus schreibt der Gesetzestext vor,

dass NSA und CIA kein Geld dafür benutzen, um Hersteller oder Anbieter dazu zu bringen, ein Produkt oder eine Dienstleistung so anzupassen, dass elektronische Überwachung ermöglicht wird.“

Vermutlich wird der Senat das Gesetz wieder aufweichen.

Das BSI hat jetzt sehr kurze Beine

Spiegel online: „Interne Berichte beschreiben etwa die Kooperation der NSA mit den deutschen Diensten und sogar mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) – das die deutschen Nutzer eigentlich vor Cyber-Bedrohungen von außen schützen sollte. (…) Vor allem aber belegt das Deutschland-Dossier die enge Zusammenarbeit zwischen NSA und BND. Nicht nur abgefangene Informationen werden geteilt: Die NSA veranstaltet Lehrgänge, man zeigt sich gegenseitig Spähfähigkeiten und tauscht untereinander Überwachungssoftware aus. So haben die Deutschen das mächtige XKeyscore bekommen, die Amerikaner durften MIRA4 und VERAS ausprobieren.“

Da bin ich jetzt aber mal gespannt. Am 26.07.2013 schrieb das BSI: „Eine Zusammenarbeit oder Unterstützung ausländischer Nachrichtendienste durch das Bundesamt für Sicherheit in der Informationstechnik im Zusammenhang mit den Ausspähprogrammen Prism und Tempora findet nicht statt. Das BSI hat weder die NSA noch andere ausländische Nachrichtendienste dabei unterstützt, Kommunikationsvorgänge oder sonstige Informationen am Internet-Knoten De-CIX oder an anderen Stellen in Deutschland auszuspähen. Das BSI verfügt zudem nicht über das Programm XKeyscore und setzt dieses nicht ein.“

Netzgemeinde oder: mit Anlauf in ihren fetten, dummen, krautgefaulten Hintern

„Aber es ist halt typisch für die aktuelle Klingelbeutelmentalität im Netz und fast immer geht es um Geld, Geld, Geld für nicht mehr als irgendwas mit Internet. Und wenn man Zweifel hat, ist man ein Spielverderber, der der Netzgemeinde schadet. Der man viel zu selten eigentlich mit Anlauf in ihren fetten, dummen, krautgefaulten Hintern tritt“. (Don Alphonso, der fast immer recht hat, wenn es um die so genannte Netzgemeinde geht.)

Heisse Luft, auch bekannt als „Cyber-Abwehrzentrum“

Sueddeutsche.de hat eine Expertise des Bundesrechnungshofes über das so genannte „Cyber-Abwehrzentrum“:

Der Rechnungshof wird sogar ziemlich grundsätzlich. Er hält die Einrichtung einer solchen Institution „nicht für gerechtfertigt“, wenn der einzig vorgegebene Arbeitsablauf die tägliche Lagebesprechung ist und „Handlungsempfehlungen auf politisch-strategischer Ebene“ nur in einem Jahresbericht gegeben würden. Es sei „fraglich“, welchen Nutzen die Einrichtung überhaupt entwickeln könne, wenn sie selbst als Informationsplattform „nur geringe Akzeptanz“ finde.

Für ihn war das Neuland

„Wenn Sie innerhalb Deutschlands eine E-Mail verschicken, ist es durchaus denkbar, dass diese über die Vereinigten Staaten und wieder zurück läuft. (…) Für mich war das neu.“ (Hans-Peter Uhl, Bundestagsabgeordneter der CSU, Mitglied im Parlamentarischen Kontrollgremium zur Kontrolle der Nachrichtendienste (!!!), in der Frankfurter Allgemeinen Zeitung).

Schöne Zitatensammlung der Süddeutschen!

Im Jahr eins nach Snowden

Lesenswert und informativ: Heise – „Was bisher geschah: Der NSA-Skandal im Jahr 1 nach Snowden“.

Truecrypt, downloaded

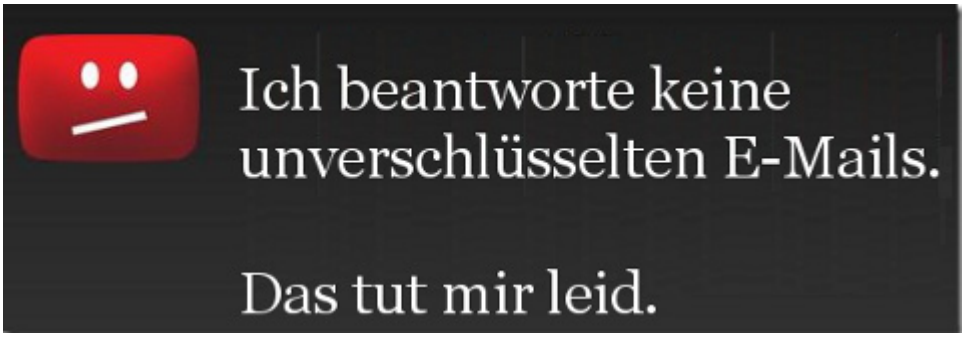
Das komplette Archiv aller aktuellen Truecrypt-Versionen ist jetzt auch auf dem Webserver der GPF, zusätzlich ein Zip-Archiv (410 MB) aller Dateien.

Not Secure As

Fefe spekuliert über Truecrypt IMHO ganz richtig (via mathew).

It smelled like a warrant canary.

Ich meine das ernst!



Manche Leute kapieren es einfach nicht….

Truecrypt, backupped

Ich habe mir noch schnell ein Backup der Truecrypt-Versionen von Heise angelegt. Vgl. Heise: „Entwickler hat angeblich Interesse verloren“.

Muahahahaha. Was für ein schlechtes Theater!

Not true crypt

Die Truecrypt-Website ist offenbar vandalisiert aka gehackt worden. Vgl. die Berichterstattung bei Heise und Fefe:

Forumsbeitrag:
If you have files encrypted by TrueCrypt on Linux: Use any integrated support for encryption. Search available installation packages for words encryption and crypt, install any of the packages found and follow its documentation.

Das sagt ja schon alles.