E-Mails verschlüsseln in 30 Minuten

Das Tutorial des Vereins *German Privacy Fund*: „E-Mails verschlüsseln in 30 Minuten“ (Alternative 2 für Windows, alles auf einem USB-Stick) wurde ~~upgedatet~~ gepatcht, ergänzt und korrigiert.

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.

Der beste Schutz: die Verschlüsselung aller Kommunikation

Heise: „Europarat hört Whistleblower Snowden an“.

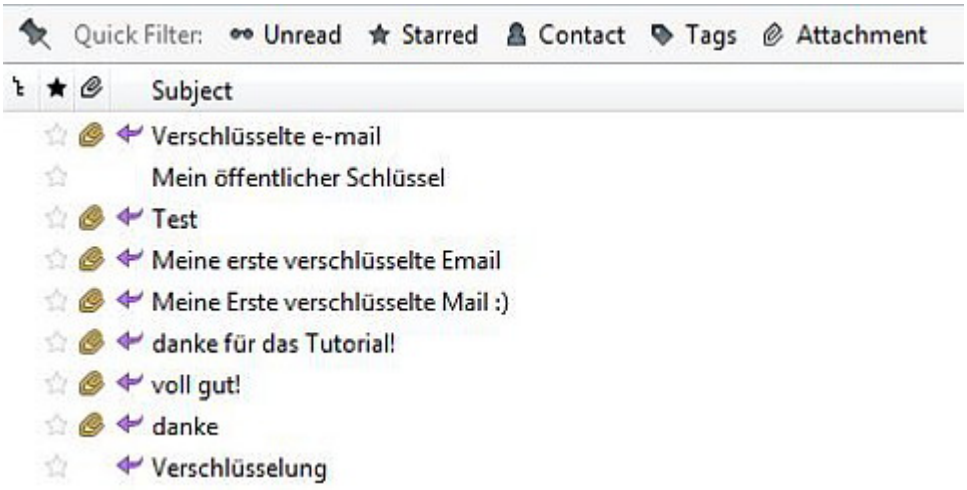
Deutsche Bürger sowie Internetseiten seien täglich Ziel der Ausspähung durch die NSA-Experten. (…) Die deutschen Dienste gehören nach Angaben des Whistleblowers neben den Niederlanden und Schweden zu den Hauptzielen von speziellen NSA-Kampagnen. (…) Snowden hält ein internationales Verbot von anlassloser Überwachung für ein wichtiges Ziel, brachte aber gleichzeitig seine Sorge zum Ausdruck, dass selbst in einer perfekten Welt der beste Schutz die Verschlüsselung aller Kommunikation sei.

Wieso kriege ich immer noch unverschlüsselte E-Mails?

German Privacy Fund

Unser Verein German Privacy Fund ist laut Bescheid des Finanzamts für Körperschaften vom 26.03.2014 gemeinnützig. Wir können also Spendenquittungen ausstellen.

Usability ist gefragt



Der Posteingang des Vereins *German Privacy Fund e.V.* wegen dieses Tutorials.

Newsletter German Privacy Fund Nr. 15

Der Newsletter German Privacy Fund (GPF) Ausgabe Nr. 15 vom 15.09.2013 ist jetzt online.

Newsletter German Privacy Fund (GPF) Nr. 15 (15.09.2013)

Der aktuelle Newsletter wurde verschickt und wird in ca. zwei Wochen auch auf der Website verfügbar sein.

Checkliste Sicherheit

Zur gefälligen Beachtung: Ich arbeite gerade an einer volkstümlichen Checkliste Sicherheit, die durch Links und Tutorials komplettiert werden soll. Wer Vorschläge hat: nur zu!

GPF Newsletter Nr. 13 (15.07.2013)

Der Newsletter German Privacy Fund (i.Gr.) Nr. 13, Ausgabe vom 15.07.2013, ist jetzt online. Der Newsletter erscheint alle zwei Wochen.

E-Mails verschlüsseln in 30 Minuten via USB-Stick

Das zweite Tutorial „E-Mails verschlüsseln in 30 Minuten“ (Windows) – alles auf einem USB-Stick – ist jetzt auch online und kann verlinkt werden.

E-Mails verschlüsseln in 30 Minuten

Das Tutorial „E-Mails verschlüsseln in 30 Minuten“ (Windows) ist jetzt alpha und online und kann verlinkt werden.

Vielen Dank allen, die Hinweise gegeben, kritisiert und auf Fehler aufmerksam gemacht haben.

Jetzt geht es ans nächste Tutorial.

E-Mails verschlüsseln in 30 Minuten Beta

Eine Beta-Version (es fehlen noch einige Links) des ersten Tutorials E-MAILS VERSCHLÜSSELN IN 30 MINUTEN ist jetzt online.

Ich bitte die geneigten Leser und wohlwollenden Leserinnen,

hier Vorschläge zu unterbreiten, was verbessert werden könnte, was unverständlich ist und wo es eventuell „hakt“.

Tutorial Beta

Die Einführung für die beiden Tutorials ist fertig.

Es kommt ein bisschen Bewegung in die Sache….[Update]

Ein Redakteur vom Berliner *Tagesspiegel* hat mir gerade seinen öffentlichen Schlüssel geschickt… Geht doch.

In ca. zwei Tagen werde ich dieses Tutorial wohl fertig haben (Windows, für Anfänger). Ich bitte alle wohlwollenden Leserinnen und geneigten Leser, die noch *nicht* ihre E-Mails verschlüsseln können, mir hier mitzuteilen, was daran unverständlich ist, was fehlt, was man besser machen könnte. (Es ist jetzt noch nicht komplett – das Wesentliche fehlt noch!)

Vermutlich werde ich daraus zwei Seiten machen. Wenn das 30-Minuten-Tutorial für blutige Anfänger fertig sein wird, mache ich mich an die Details und an die anderen Features, danach kommen S/Mime, Verschlüsseln mit Linux und Mac usw..

[Update]: bei Spiegel online gibt es ein nettes Tutorial – ich

musste schmunzeln, weil ich gerade fast identische Screenshots gemacht hatte…

GPF-Newsletter Nr. 12

Der Newsletter German Privacy Fund (i.Gr.) Nr. 12, Ausgabe vom 02.07.2013, ist erschienen. Der Newsletter erscheint jetzt alle zwei Wochen.

GPF Newsletter Juni 2013

GPF Newsletter Juni 2013 – Auszug:

Abschnitt Eins: In Eigener Sache

Der Verein German Privacy Foundation e.V. löst sich auf. (Mehr dazu in „GPF intern“) Der Newsletter wird weiter monatlich erscheinen.
Er wird redaktionell betreut von Albrecht Ude und Burkhard Schröder und ab der Ausgabe 12 (Juli 2013) jeweils am Monatsanfang von einem neuen Verein herausgegeben werden, der von ehemaligen Mitgliedern und Sympathisanten der German Privacy Foundation gegründet worden ist.

Sie müssen diesen Newsletter neu abonnieren, da wir aus Gründen des Datenschutzes die Abonnenten nicht einfach übertragen wollen und können.

Abonnement des Newsletters über die Mailingliste des Vereins „German Privacy Fund“ (GPF): listserv.burks.de/mailman/listinfo/gpf

Der Volltext des GPF Privacy Newsletters ist hier archiviert. Dort werden auch die nächsten (monatlichen) Ausgaben zu finden sein.

Der Twitter-Account: GPF_ev wird vom neuen Verein genutzt werden.
https://twitter.com/gpf_ev

Verantwortlich für alle zukünftigen Inhalte des Newsletters (V.i.S.d.P. und Verantwortliche (gemäss § 5 TMG): Burkhard Schröder und Albrecht Ude .

Die Redaktion erreichen Sie mit einer E-Mail an: newsletter@german-privacy-fund.de oder info@german-privacy-fund.de .

German Privacy Foundation ff.

Die Mitgliederversammlung des Vereins *German Privacy Foundation* hat in der letzten Woche einstimmig beschlossen, den Verein aufzulösen. Aus der Begründung:

Zeitmangel der Vorstandsmitglieder
Wir haben festgestellt, daß wir Vorstandsmitglieder mehrheitlich kaum noch Zeit für GPF-Projekte aufbringen können. Wir sind zwar durchaus noch in der Lage, den Verein zu verwalten und den dafür üblichen Anforderungen zu genügen. Wir haben aber inzwischen einfach zu wenig Ressourcen, unsere Angebote ausreichend zu betreuen und neue Projekte zu entwickeln.

Abschaltung der PrivacyBox
Das gilt besonders für die PrivacyBox. Die werden wir in den nächsten Monaten aus verschiedenen Gründen einstellen (siehe unten). Wir haben das bereits auf der letzten MV im September beschlossen, allerdings glaubten wir damals, bis dahin eine neue Version des Systems entwickeln zu können. Leider fehlt uns dazu leider nun doch die Zeit und eine baldige Lösung ist nicht in Sicht. Eines unserer zentralen Projekte fällt damit ersatzlos weg. Es gibt aber bereits freie wie kommerzielle Projekte mit ähnlicher Ausrichtung und wir denken, daß diese sich auch ohne unser Zutun gut entwickeln können.

Anonymisierungsdienste
Wir haben die Angebote der GPF an Anonymisierungsdiensten – vor allem Tor-Servern – seit der Gründung 2007 ausgebaut und bis jetzt stets zuverlässig betrieben. Unser Tor-Partnerprogramm hat sich als Modell auch in anderen Vereinen etabliert. Die hatten oder haben inzwischen mehr Aktive und größere Ressourcen als wir, weshalb wir denken, daß wir unsere Aktivitäten einstellen können, ohne eine große Lücke zu hinterlassen. (…)

CryptoStick

Außerdem müssen wir natürlich etwas zum CryptoStick schreiben: Das Projekt lebt und wird noch immer weiterentwickelt. Es war jedoch von Beginn an nur teilweise in der GPF verankert. Seit längerem hat es eigene Website und der Stick wird nicht mehr vom Verein vertrieben. Eine Auflösung der GPF würde den CryptoStick also nicht gefährden.

Von Mitgliedern der alten GPF und deren Freunden wurde ein neuer Verein mit ähnlichem Konzept und Namen gegründet, der in Kürze in das Vereinsregister eingetragen werden wird. Dieser Verein wird den Privacy-Newsletter fortführen und das Archiv der GPF-Website verfügbar halten, ist aber kein Rechtsnachfolger.

Mitgliederdaten oder andere interne Unterlagen der GPF werden dem neuen Verein nicht übergeben. Der GPF-Newsletter muss also neu abonniert werden. In der nächsten Ausgabe wird stehen, wo und wie.

Wir empfehlen denjenigen von euch, die Tor-Server betreiben oder ihren Betrieb unterstützen wollen, ein Engagement bei den Zwiebelfreunden.

Wer Ersatz für die Privacybox sucht, wird vielleicht bei der ZEIT fündig, dort gibt es seit einigen Monaten einen digitalen Briefkasten mit frei verfügbarem Quellcode.

Wer am Cryptostick interessiert ist oder Support dafür braucht, kann sich auf der Projektwebsite informieren.

Vorsitzende des neuen Vereins sind Albreecht Ude von *Netzwerk Recherche* und ich.

Anonym Mails empfangen?

```
From burks@burks.de Tue Apr 30 12:03:23 2013
Return-Path: <burks@burks.de>
Delivered-To: 8c150e57cb1e-e3d91cff13e1@8c150e57cb1e.anonbo
Received: (qmail 47885 invoked by uid 0); 30 Apr 2013 12:03
Received: from unknown (HELO mail.minuskel.de) (193.96.188.
  by anonbox.net with AES256-SHA encrypted SMTP; 30 Apr 201
Received: from p57b99c14.dip0.t-ipconnect.de ([87.185.156.2
        by mail.minuskel.de with esmtpsa (TLSv1:AES256-SHA:
        (Exim 4.43)
        id 1UX9HG-0004py-Ct
        for e3d91cff13e1@8c150e57cb1e.anonbox.net; Tue, 30
Message-ID: <517FB309.8020508@burks.de>
Date: Tue, 30 Apr 2013 14:03:21 +0200
From: Burkhard Schroeder <burks@burks.de>
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:17.0) Ge
MIME-Version: 1.0
To: e3d91cff13e1@8c150e57cb1e.anonbox.net
Subject: testmail
X-Enigmail-Version: 1.5.1
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: 7bit

bla
```

Da die Privacybox der GPF demnächst abgeschaltet wird, suche ich nach einer Alternative.

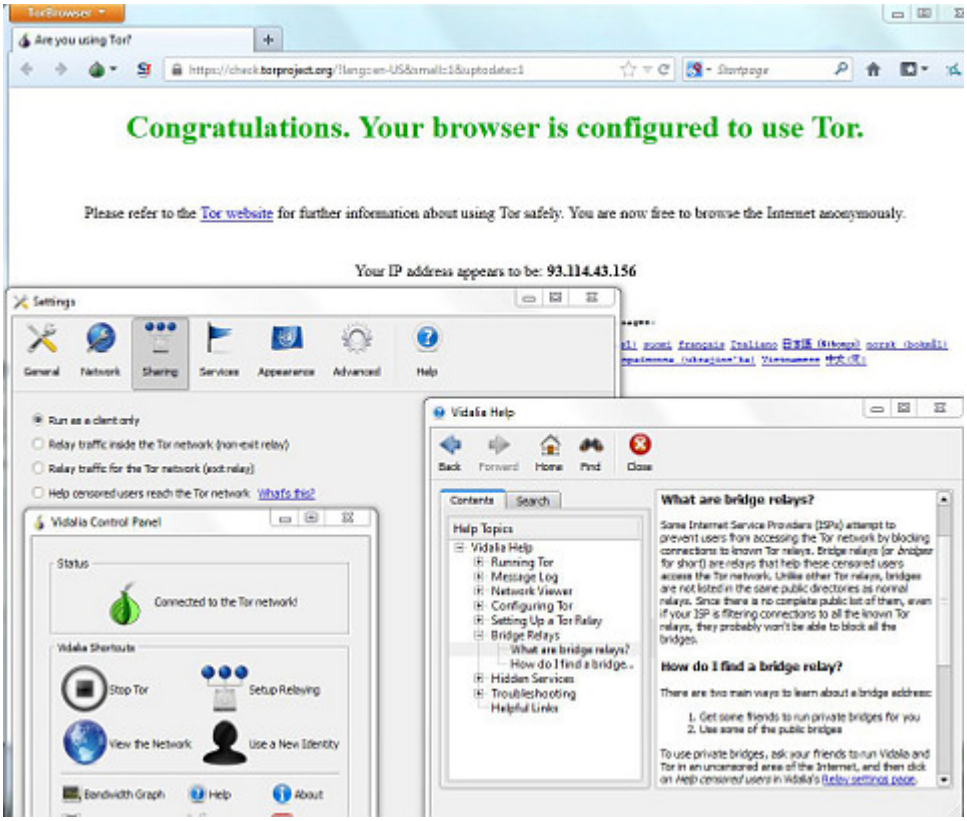
Anonbox.net vom CCC verstehe ich nicht: Wenn ich mir an meinen temporär erzeugten Account eine Mail schreibe, sehe ich, woher sie kommt – das ist doch das Gegenteil von dem, was ich erreichen will? Oder denke ich irgendwie um die Ecke?

Erstens will ich mich auch nicht immer mit dem Zertifikat herumärgern, zweitens schalte ich Javascript natürlich *nicht* ein (was man aber nicht unbedingt tun muss, vgl. Sceenshot), drittens würde ich gern die Mails auch noch automatisch verschlüsselt empfangen.

Bei awxcnx.de kann man sich auch keinen eigenen Account einrichten.

Kennt jemand eine Lösung, ein Interface in eine Website einzubauen?

Unter Zwiebelfreunden



Nur zur Erinnerung: Anonym surfen ist keine Wissenschaft für Geeks, sondern ganz simpel, auch für technisch unbedarfte Windows-NutzerInnen! Einfach ausprobieren – für's „Zweitsurfen" sozusagen. Heutzutage hat jeder normale PC soviel Arbeitsspeicher, dass man mehrere Browser benutzen kann, zur Not auch parallel.

1. Schritt: den Tor-Browser Bundle herunterladen und installieren. (Ich habe alles in Englisch hier, aber die Software gibt es auch auf Deutsch.)

2. Wenn man dann die „Executable" (.exe =das Programm) ausführt, sollte zunächst das Menü der grafischen Oberfläche Vidalia erscheinen, während der eigentliche Browser noch hochfährt.
Vidalia lets you start and stop Tor, see how much bandwidth

you are consuming, see how many circuits you currently have active, see where these circuits are connected on a global map, view messages from Tor about its progress and current state, and let you configure your Tor client, bridge, or relay with a simple interface. Included in Vidalia is an extensive help system which helps you understand all of the options available to you. All of these features are translated into a large number of languages.

3. Surfen!

4. Mal in den Optionen von Vidalia herumklicken (vgl. Screenshot). Zum Beispiel lernen, was Tor Bridges sind:
Bridge relays (or „bridges“ for short) are Tor relays that aren’t listed in the main Tor directory. Since there is no complete public list of them, even if your ISP is filtering connections to all the known Tor relays, they probably won’t be able to block all the bridges. If you suspect your access to the Tor network is being blocked, you may want to use the bridge feature of Tor. The addition of bridges to Tor is a step forward in the blocking resistance race. It is perfectly possible that even if your ISP filters the Internet, you do not require a bridge to use Tor. So you should try to use Tor without bridges first, since it might work.

4. Wer sich langweilt, kann die FAQ (Häufig gestellten Fragen) durchlesen und anschliessend seinem sozialen Umfeld erklären, was ein wahrer Zwiebelfreund ist.

By the way: Die gemeinnützige German Privacy Foundation betreibt mehrere Tor-Server. Man kann in den Verein eintreten und das unterstützen!

GPF Newsletter Nr. 9

Der GPF Newsletter Nr. 9 – Ausgabe vom 20.3.2013 ist erschienen.