Tails

theamnesicincognitolivesystem

Erste Hinweise und Erklärungen zu einem Live-Betriebssystem, das Ihre Privatsphäre schützen und eine vertrauliche, verschlüsselte Kommunikation ermöglichen soll.

https://tails.boum.org/index.de.html

Privatsphäre für jeden, überall

Tails ist ein Live-Betriebssystem, das Sie auf auf vielen Computern von einer DVD, einem USB-Stick oder einer SD-Karte aus starten können. Es zielt darauf ab, Ihre Privatsphäre und Anonymität zu bewahren und hilft Ihnen:

- das Internet anonym zu nutzen und Zensur zu umgehen;
- alle Verbindungen zum Internet werden zwingend durch das Tor Netzwerk geleitet oder geblockt;
- auf dem verwendeten Computer keine Spuren zu hinterlassen, sofern Sie es nicht ausdrücklich wünschen;
- kryptographische Werkzeuge auf dem aktuellen Stand der Technik zu benutzen um Ihre Dateien, E-Mails und Instant-Messaging-Nachrichten zu verschlüsseln.

Erste Schritte ...

Ist Tails das richtige Werkzeug für mich?

1. Lesen Sie zunächst "Über Tails", um eine grundlegende Vorstellung davon zu bekommen, was Tails ist.

2. Lesen Sie danach die "Warnungen", um zu verstehen wogegen Tails Sie nicht schützen kann, wie Sie Ihre Anonymität verlieren oder Spuren hinterlassen können.

3. Sollte Tails das richtige Werkzeug für Sie sein, können Sie es im Internet unter https://www.tails.boum.org/index.de.html herunterladen, verifizieren und installieren.

4. Wenn Sie Tails benutzen, ist es sehr wichtig in Sicherheitsfragen und neuen Versionen auf dem aktuellen Stand zu bleiben.

Über Tails

> **Amne|sie** (die; -, Nomen)
> [gr.-nlat.: a „ohne, nicht“, mnesis „Erinnerung“]
> Form des Gedächtnisschwunds; bspw.: Verlust des Langzeitgedächtnisses.
>
> **in|kọ|gni|to** (Adverb / das; -, Nomen)
> [lat.-it.: in- (verneinend), cognoscere „erkennen; bemerken“]
> Einer Person: unter fremdem Namen auftretend; unidentifizierbar.

Tails ist ein Live-Betriebssystem, das darauf ausgerichtet ist Ihre Privatsphäre und Anonymität zu bewahren. Es hilft Ihnen dabei, das Internet so gut wie überall und von jedem Computer aus anonym zu nutzen, ohne dabei Spuren zu hinterlassen, sofern Sie dies nicht ausdrücklich wünschen.

Tails ist ein vollständiges Betriebssystem, das direkt von einer DVD, einem USB-Stick oder einer SD-Karte aus genutzt wird, unabhängig von dem auf dem Computer installierten Betriebssystem. Tails ist Freie Software und basiert auf Debian GNU/Linux.

Tails beinhaltet verschiedene Programme, die im Hinblick auf die Sicherheit vorkonfiguriert wurden: einen Webbrowser, einen Instant-Messaging-Client, ein E-Mail-Programm, ein Office-Paket, einen Bild- und Audioeditor etc.

Anonymität online und Zensurumgehung mit Tor

Tails verlässt sich auf das Anonymisierungsnetzwerk Tor, um Ihre Online-Privatsphäre zu schützen:

- Sämtliche Software ist so konfiguriert, dass sie sich über Tor mit dem Internet verbindet.
- Falls eine Anwendung versucht, sich direkt mit dem Internet zu verbinden, wird die Verbindung zur Sicherheit automatisch geblockt.

Tor ist Freie Software und ein offenes Netzwerk, das Ihnen dabei hilft, sich gegen eine Form der Netzwerküberwachung zu wehren, die persönliche Freiheit und Privatsphäre, vertrauliche Geschäftsbeziehungen, und die Sicherheit von Ländern gefährdet: die sogenannte »Verkehrsdatenanalyse«.

Tor schützt Sie, indem es Ihre Kommunikation durch ein verteiltes Netzwerk von Relais springen lässt, das von Freiwilligen aus aller Welt betrieben wird. Es verhindert, dass jemand der Ihre Internetverbindung beobachtet, nachvollziehen kann, welche Seiten Sie besuchen, und sorgt dafür, dass die von Ihnen besuchten Seiten Ihren tatsächlichen Standort nicht ausfindig machen können.

Mit Tor können Sie:

- Durch das Verschleiern Ihres Standortes online anonym sein.
- Sich mit Diensten verbinden, die andernfalls zensiert wären.
- Angriffen widerstehen, die Tor blockieren, durch den Einsatz von Umgehungssoftware wie den Tor-Bridges (Brücken in das Tor-Netzwerk).

Mehr über Tor erfahren Sie auf der offiziellen Webseite des Tor-Projekts:

https://www.torproject.org/

Überall nutzen, ohne Spuren zu hinterlassen

Die Benutzung von Tails auf einem Computer verändert weder das installierte Betriebssystem, noch ist es von diesem abhängig. Es kann also gleichermaßen auf dem eigenen Computer, dem eines Freundes, oder einem Computer der örtlichen Bibliothek verwenden werden. Nachdem Sie Tails heruntergefahren haben, kann der Computer wie gehabt mit seinem üblichen Betriebssystem starten.

Tails ist mit großer Sorgfalt konfiguriert nicht die Festplatten des Computers zu benutzen, auch nicht wenn Auslagerungsspeicher (swap space) zur Verfügung steht. Der einzige von Tails genutze Speicher ist der Arbeitsspeicher (RAM), der automatisch gelöscht wird, sobald der Computer herunterfährt. So hinterlassen

sie weder Spuren des Tails-Systems, noch dessen, was Sie auf dem Computer getan haben. Deshalb nennen die Entwickler Tails "amnestisch" (engl.: amnesic).

Dies erlaubt Ihnen auf jedem Computer an sensiblen Dokumenten zu arbeiten, und schützt Sie vor Datenwiederherstellung nach dem Herunterfahren. Natürlich können Sie weiterhin ausgewählte Dokumente und Dateien auf einem anderen USB-Stick oder einer externen Festplatte speichern, und für die zukünftige Nutzung mit sich nehmen.

Kryptographische Werkzeuge auf dem aktuellen Stand der Technik

Tails beinhaltet eine Auswahl an Werkzeugen, um Ihre Daten mit starker Verschlüsselung zu schützen:

- Verschlüsseln Sie Ihren USB-Stick oder externe Festplatten mit LUKS, dem Linux-Standardprogramm zur Festplattenverschlüsselung.
- Verschlüsseln Sie mit HTTPS Everywhere Ihre Kommunikation mit einer Vielzahl großer Webseiten automatisch durch HTTPS. HTTPS Everywhere ist ein Firefox-Plugin, welches von der Electronic Frontier Foundation entwickelt wird.
- Verschlüsseln und signieren Sie Dokumente und E-Mails mit dem de facto Standard OpenPGP, entweder in Tails E-Mail-Client, dem Text-Editor oder aus dem Datei-Browser heraus.
- Schützen Sie Ihre Unterhaltungen über Instant Messaging (IM) mit OTR - ein kryptographisches Protokoll, welches Verschlüsselung und Authentifizierung bietet, sowie dem Prinzip der glaubhaften Abstreitbarkeit (plausible deniability) folgt.
- Löschen sie Ihre Dateien auf sichere Art und Weise und überschreiben Sie Ihre Festplatte mit Nautilus Wipe.

System-Voraussetzungen

Tails sollte auf so gut wie jedem halbwegs aktuellen Computer laufen (d.h. jünger als 10 Jahre). Folgende Voraussetzungen muss der Rechner jedoch erfüllen:

- Ein internes oder externes DVD-Laufwerk, oder die Möglichkeit von einem USB-Stick oder einer SD-Karte zu starten.
- Tails benötigt einen Prozessor, der auf der x86-Architektur basiert. Deshalb läuft es auf den meisten gängigen IBM-PC-kompatiblen Computern (z. B. Windows-PCs), aber nicht auf PowerPC- oder ARM-Rechnern. Mac-Computer sind seit 2006 auch kompatibel zu IBM-PCs.
- Tails braucht 1GB RAM, um sauber zu arbeiten. Notfalls läuft es auch mit weniger Arbeitsspeicher, allerdings kann es dann zu unerwarteten Störungen oder Systemabstürzen kommen.

Warnhinweise!

Obwohl die Tails-Entwickler ihr Bestes geben, um Ihnen gute Werkzeuge anzubieten, die Ihre Privatsphäre während der Benutzung eines Computers schützen, gibt es keine Magie und keine perfekte Lösung zu einem solch komplexen Problem. Die Grenzen dieser Werkzeuge zu verstehen, ist ein sehr wichtiger Schritt, um erstens zu entscheiden, ob Tails das Richtige für Sie ist, und zweitens hilft es Ihnen Tails sinnvoll einzusetzen.

1. Tor Austritts-Knoten können Verbindungen abhören - daher sollten sie möglichst immer https-Verbindungen bevorzugen und Ende zu Ende-Verschlüsselung, wo möglich, nutzen.
2. Tails offenbart, dass Sie Tor benutzen und vermutlich auch, dass Sie ein Tails-Benutzer sind.
3. Man-in-the-middle-Angriffe sind möglich – kommunizieren Sie deswegen möglichst immer nur verschlüsselt.
4. Angriffsszenarien bei vollüberwachtem Internetverkehr mittels Traffic-Analyse sind denkbar.

5. Die Verschlüsselung von abgespeicherten Dateien ist bei Tails nicht standardmäßig eingeschaltet.
6. Tails sorgt nicht automatisch für das Entfernen von Metadaten aus Dokumenten, Bildern und anderen Dateien und die Betreff-Zeile von E-Mails bleiben stets unverschlüsselt.
7. Tor bietet keinen Schutz im Fall von flächendeckender Überwachung des Internetverkehrs.
8. Tails kann nicht dafür sorgen, verschiedene Identitäten voneinander zu trennen. Sie sollten daher z.B. nicht zeitgleich bei Diensten wie bspw. Facebook angemeldet sein.
9. Tails ist unfähig, die Probleme von schlechten oder schwachen Passwörtern zu beheben.
10. Tails ist niemals fertig und wird ständig weiter entwickelt - es kann auch für Tails keine Garantie auf unbekannte Sicherheitslücken geben.

Ausführliche Erläuterungen zu jedem dieser Punkte/Risiken gibt es auf der Homepage von Tails.

Tails ist in den Standardeinstellungen ein sorgsam und gut konfiguriertes System. Beachten Sie, dass Änderungen daran, wie die Deaktivierung von Javascript, die Installation weiterer Browser-Plugins (oder das Abrufen Ihrer privaten Emails) Ihre Anonymität schwächen kann.

Mitgelieferte Programme

Tails ist eine umfangreiche und gut durchdachte Zusammenstellung freier Software.

Nach der Installation bzw. nach dem Start stehen Ihnen unter anderem folgende Programme zur sofortigen Benutzung zur Verfügung:

- GNOME, eine intuitive und attraktive Desktop-Umgebung für Linux-Betriebssysteme
- Tor, ein Tool zur Anonymisierung von Internetverbindungen

- Firefox vorkonfiguriert mit:
    - TorBrowser-Korrekturen
    - Torbutton für Anonymität und Schutz gegen böses JavaScript
    - alle Cookies werden standardmässig als Session-Cookies behandelt;
    - HTTPS Everywhere aktiviert SSL-verschlüsselte Verbindungen zu einer grossen Anzahl von bekannten Webseiten
    - NoScript für noch mehr Kontrolle über JavaScript
    - AdBlock Plus um Werbung zu entfernen
- Pidgin vorkonfiguriert mit OTR Off-the-Record Messaging (Verschlüsselung von Instant-Nachrichten)
- Claws Mail, ein E-Mail-Programm mit GnuPG-Unterstützung
- Gobby zum kollaborativen Schreiben von Texten
- I2P ein Anonymisierungsnetzwerk (Achtung: In der aktuellen Version Tails 1.1 mit Sicherheitslücke – nicht benutzen!)
- LibreOffice, die vollständige Suite für Textverarbeitung, Tabellenkalkulation und Präsentationen
- Gimp und Inkscape zum Bearbeiten von Bildern
- Scribus, ein Layout-Programm
- Audacity zum Aufnehmen und Bearbeiten von Sound
- PiTiVi zur nicht-linearen Audio-/Videobearbeitung
- Brasero zum Brennen von Cds/DVDs
- LUKS und Palimpsest zum Installieren und Nutzen verschlüsselter Speichermedien, wie zum Beispiel USB-Sticks
- GnuPG, die GNU-Implentierung von OpenPGP zum Verschlüsseln und Unterschreiben von E-mails und Daten
- TrueCrypt, ein Programm zur Festplattenverschlüsselung
- PWGen, ein Generator für starke Passwörter
- Florence, eine virtuelle Tastatur zum Schutz gegen Hardware-Keylogger
- MAT zum Anonymisieren von Metadaten in Dateien
- KeePassX ein Passwortmanager
- und viele weitere mehr ...

Weitere Merkmale von Tails

- Tails beinhaltet einen automatischen Mechanismus zum Aktualisieren des USB-Sticks oder der SD-Karte auf eine neuere Version.
- Tails kann als virtuelle Maschine in VirtualBox ausgeführt werden.
- Individuelles Anpassen (d.h. ein fehlendes Stück Software hinzuzufügen) ist relativ leicht: ein eigenes Amnesic Incognito Livesystem kann in ca. einer Stunde auf einem modernen Rechner eigens erstellt werden.
- Tails hält standardmäßig einige simple Barrierefreiheit-Features bereit.

Um Cold-Boot-Attacken und diverse Computer-Forensiktechniken zu verhindern, löscht Tails den Arbeitsspeicher beim Herunterfahren und wenn das Startmedium entfernt wird.

Herunterladen, prüfen und Installieren von Tails

Hinweise zur Installation sowie den Direktlink zum Download von Tails gibt es hier:

https://tails.boum.org/download/index.de.html

Darüber gelangt man an eine heruntergeladene Datei mit der .iso-Endung. Nach Überprüfung der Echtheit (Integrität) der herunter geladenen Datei kann man diese iso-Datei mittel eines Hilfsprogramms beispielsweise auf einem USB-Stick installieren, um dann damit mit Tails starten zu können.

Mit dem Programm UNetbootin (gibt es für Linux, Windows und Mac OS X) kann man damit einen Live-USB-Stick mit dem Tails-System darauf erzeugen:

http://unetbootin.sourceforge.net/

Bitte unbedingt die weiteren Hinweise auf der Homepage von Tails beachten:

https://tails.boum.org/doc/first_steps/index.de.html

Kann ich Tails vertrauen?

Vetrauen ist ein sehr heikle Sache. Dies ist die Essenz warum auch Sicherheit an und für sich eine schwierige Sache ist. Computer und Internet Kommunikation stellen hier keine Ausnahme dar. Vertrauen Sie Tails und seinen Entwicklern? Glauben Sie, dass die Tails-Entwickler Backdoors eingebaut haben, um Kontrolle über Ihrern Computer übernehmen zu können? Oder das die Tails-Entwickler kompromittierte Verschlüsselungs-Keys erzeugen damit die Regierung Sie ausspionieren kann? Vertrauen Sie auf diese Aussagen oder wollen Sie Beweise?

Wie auch immer Ihre Meinung zu diesem Thema ist, Sie sollten sich selber Fragen, wie Sie zu dieser Meinung gekommen sind. Vertrauen und Misstrauen müssen auf Fakten basieren und nicht auf dem Bauchgefühl, paranoiden Verdächtigungen, unbelegbarem Hörensagen oder dem von Tails-Entwicklern gegebenen Wort. Natürlich behaupten diese ehrlich zu sein aber diese Behauptung ist unter dem Strich wertlos. Um eine fundierte Entscheidung treffen zu können, müssen Sie das große Ganze von Tails betrachten, sich mit den Mitgliedern der Tails-Entwickler-Gemeinschaft und deren Organisation vertraut machen, sowie möglicherweise mit Einbeziehen, in welcher Form andere Nutzer diesem System vertrauen.

Im Einzelnen:

Freie Software and öffentliche Überprüfung

Freie Software, wie Tails ermöglicht es seinen Benutzern genau zu überprüfen, woraus die einzelnen Softwarebausteine bestehen und wie die einzelnen Bausteine miteinander interagieren, da der Quellcode für jeden interessierten Nutzer frei zur Verfügung gestellt werden muss. Eine gründliche Code-Überprüfung bringt schädlichen Code, wie eine Backdoor, zu Tage. Darüber hinaus ist es möglich die Software selber zu übersetzen und anschließend mit der bereitgestellten Version, wie den Tails ISO Images, zu vergleichen. Auf diesem Weg kann überprüft werden, ob die bereitgestellte Version von der gleichen Codebasis erzeugt oder ob schadhafter Code eingeschmuggelt wurde.

Natürlich haben die meisten Nutzer entweder zu wenig Detailwissen, technische Fähigkeiten oder schlichtweg keine die Zeit, um dies zu tun. Durch die öffentliche

Prüfbarkeit kann aber freier Software ein gewisser Grad an Vertrauen per se entgegen gebracht werden. Zumindest, wenn die Software ein gewisse Popularität genießt, kann man davon ausgehen, dass andere, nicht am Projekt beteiligte Entwickler, in den Quellcode geschaut haben. Zusätzlich besteht eine lange Tradtion in der Free Software Community, grobes Fehlverhalten von Software öffentlich anzuprangern.

Debian GNU/Linux vertrauen

Der Großteil der gesamten Software, die mit Tails verteilt wird, stammt aus der Debian GNU/Linux Distribution. Debian ist mutmaßlich die Linux Distribution, deren Packages am intensivsten auditiert werden. Nicht nur, dass Debian eine der größten Linux Distributoren ist, sondern es ist auch die populärste Basis-Distribution, um eigene, angepasste Distributionen zu erzeugen. Als Beispiel sei hier Ubuntu genannt, sowie dessen Ablegern, wie Linux Mint. Deshalb benutzen unzählige Nutzer Debian's Software Pakete und unzählige Entwickler prüfen deren Integrität. Zwar wurden ernste Sicherheitslücken entdeckt (wie die berühmt-berüchtigte Debian SSH PRNG vulnerability) aber, soweit bekannt, niemals Backdoors oder andere Arten von absichtlichen Sicherheitslücken.

Tor vertrauen

Tails Anonymiserungsfähigkeiten basieren auf Tor, welches von `The Tor Project` entwickelt wird. Die Entwicklung findet unter großer öffentlichen Auditierung statt - sowohl aus akademischer (Forschung bezüglich Angriffsvektoren und Verteidigungsmaßnahmen beim Onion-Routing) als auch softwaretechnischer Sicht (der Quellcode wurde diversen externen Audits unterzogen, sowie von vielen unabhängigen Software-Entwicklern aus diversen Gründen gelesen). Auch hier wurden Sichheitsrisiken gefunden, aber keinerlei Backdoors oder anderer schadhafter Code - nur uninformierte Verschwörungstheoretiker spekulieren heutzutage über Backdoors in Tor. Darüber hinaus macht es das verteilte Vertrauensmodell, welchem Tor zugrunde liegt, sehr schwer für einen einzelnen Tor-Knoten, den einzelnen Datenverkehr auszuspähen, geschweige denn eine Person zu identifizieren.
Allerdings: Die Benutzung von Tor erfreut sich zunehmender Beliebtheit und ist fast so etwas wie ein Quasi-Standard für IP-Verschleierung beim Internet-Surfen

geworden. Das bedeutet zugleich, dass staatliche oder geheimdienstliche Anstrengungen zur Deanonymisierung von Tor-Nutzern verstärkt werden - darüber sollten Sie sich bewusst sein (siehe auch die Warnhinweise S. 6/7).

Fazit

Man könnte sagen, dass Tails die Vereinigung von Debian und Tor ist. Im Groben gesagt verbinden die Tails-Entwickler die beiden Welten mit dieser Distribution. Demzufolge - wenn Sie Debian und Tor vertrauen sollten - müssen Sie nur noch dieser "Verbindung" vertrauen, um auch Tails trauen zu können. Wie schon gesagt ist Tails Free Software. Der Quellcode liegt offen und besteht hauptsächlich aus einer Liste zu installierender Debian Pakete nebst Ihrer Konfiguration. Tails steht sicherlich nicht so stark im Fokus, wie Debian und Tor es tun, aber dennoch hat es einige Aufmerksamkeit im Umfeld der Tor Community, so wie bei einigen Sicherheit Communities. Tails' Quellcode ist ziemlich überschaubar und unkompliziert. Deshalb ist die Tails-Entwickler-Gemeinschaft stärker im Fokus als viele andere Projekte, die den selben Zweck verfolgen.

Nachdem das nun gesagt ist (und was Sie idealer Weise selber auf seinen Wahrheitsgehalt überprüft haben), sollten Sie nun in der Lage sein, eine fundierte Entscheidung darüber treffen zu können, ob Sie Tails vertrauen können.

Lizenzen und weitere Informationen

Tails ist Freie Software, die unter der GNU General Public License (Version 3 oder höher) veröffentlicht wurde.

Viele weitere wichtige Informationen gibt’s auf der Homepage von Tails.

Ein gutes und sehr ausführliches Tails-Handbuch in deutscher Sprache gibt es bei:

https://capulcu.nadir.org/

Dieses Heftchen wurde von freiheitsfoo erstellt und beruht in großen Teilen auf von der Tails-Homepage bereit gestellten Texten. Mehr Infos zu freiheitsfoo gibt es auf **www.freiheitsfoo.de**
07/2014