Tipps für sichere Kommunikation

1. Verschlüssele deine Computer / Handy

Windows: Truecrypt | Mac OSX: FileVault 2 | Linux: bei Installation Verschlüsselungsoption auswählen | Android: Systemeinstellungen

2. Sperre deinen Bildschirm mit einem Passwort um unerlaubten Zugriff auf deinen Computer/Handy zu verhindern

3. Benutze einen Passwortmanager (z.B. KeepassX)

4. Verschlüssele deine Kommunikation

- SMS: Textsecure (Android)
- Mobiltelefonie: Redphone (Android) ; Signal (iOS)
- Email: Thunderbird mit GPG und Enigmail-Plugin
- Surfen: Browser-Plugin HTTPS Everywhere
- Chat: Pidgin (Windows, Linux) , Adium (Mac OSX) jeweils mit OTR-Plugin

5. verwende zum anonymen Surfen den Tor-Browser

6. Suche dir vertrauenswürde Dienstanbieter

z.B. https://systemli.org/service/index.html

Um viele dieser Programme auszuprobieren, kannst du die Live-CD Tails verwenden, ohne die Programme auf deinem Rechner installieren zu müssen.

OpenSource vs. Closed Source:

Der Quellcode eines Programms wird im englischen auch als Source Code bezeichnet. Software deren Quellcode der Welt offen steht - das heißt jeder kann ihn lesen, ändern oder erweitern – wird als Open Source bezeichnet. Mit Closed Source wird Software bezeichnet, bei der der Source Code nicht öffentlich zugänglich ist. Der Benutzer kann das Programm nur installieren und anwenden. Es sind keine Änderungen im Code oder Überprüfung der Funktionsweise möglich.

eMail

Thunderbird

Thunderbird ist ein OpenSource Emailprogramm. Mit der Erweiterung Enigmail ist es sehr einfach möglich Emails zu ver- und entschlüsseln oder zu signieren.

GPG/PGP

GPG/PGP wird hauptsächlich verwendet um Emails zu verschlüsseln. GPG ist die freie Version der PGP-Software, die mittlerweile einer Firma gehört und keine OpenSource-Software mehr ist.

GPG basiert auf einer Art Schlüssel-Schloss-Prinzip. Jeder Teilnehmer einer Kommunikation besitzt einen öffentlichen Schlüssel, einen privaten Schlüssel und ein Passwort. Der private Schlüssel und das Passwort sind nur ihm bekannt. Der öffentliche Schlüssel kann je nach Lust und Laune an Freund_innen, Kommunikationspartner_innen oder das Internet verteilt werden. Möchten zwei Teilnehmer_innen (A und B) miteinander verschlüsselt kommunizieren, benötigen sie den öffentlichen Schlüssel des Gegenübers. Kommunikationspartner A verschlüsselt nun einen Text oder eine Datei mit Hilfe bzw. auf den öffentlichen Schlüssel von Kommunikationspartner B. Der Text/die Datei ist so verschlüsselt, dass er nur mit Hilfe des zugehörigen privaten Schlüssels und dem Passwort von Kommunikationspartner B geöffnet bzw. die Datei entschlüsselt werden kann.

Win: GPG4Win, Mac: gpgtools, Linux: standardmäßig installiert

Chat

Pidgin (Windows/Linux) + OTR

Pidgin ist ein OpenSource InstantMessaging Programm, das viele verschiedene Chat-Protkolle (Jabber/XMPP, ICQ, MSN, IRC ...) beherrscht. Mit dessen Hilfe kannst du mit deinen Freunden und Freundinnen über einen Server deiner Wahl chatten. Es ist sowohl für Windows und Linux verfügbar. Mit Hilfe eines Plugins ist es möglich, die sogenannte OTR-Verschlüsselung nachzurüsten. Andere OpenSource InstantMessaging Programme sind zum Beispiel Psi oder Gajim.

Adium + OTR (Mac OS X)

Adium ist ein OpenSource InstantMessaging Programm, das viele verschiedene Chat-Protkolle (Jabber/XMPP, ICQ, MSN, IRC ...) beherrscht. Es ist lediglich für Mac OS X vrefügbar. Es beherscht von Haus aus das sogenannte OTR-Protokoll für Ende-zu-Ende verschlüsselte Kommunikation.

Off the record

OTR

OTR ist die Kurzform für das sogenannte Off-the-Record-Messaging (zu deutsch: inoffizielle; vertrauliche, nicht für die Öffentlichkeit bestimmte Nachrichtenvermittlung). Es ist ein Verschlüsselungsprotokoll, dass die Instant-Messaging-Kommunikation (Jabber, ICQ, IRC uvm.) zwischen zwei Parteien Ende-zu-Ende verschlüsselt.

Die Nutzung von OTR ist anzuraten, da zwischen den beiden Parteien immer ein Vermittler (der Server) arbeitet, der die Kommunikation der beiden Parteien mitlesen kann, da die Mitteilungen dort vor dem Weiterversand kurz ent- und wieder verschlüsselt werden. Auch ein Angreifer könnte sich zwischen Kommunikationspartner A und Server schalten und versuchen die Gespräche abzufangen. Dies ist besonders einfach, wenn der Server nicht auf die sogenannte SSL-Verschlüsselung besteht.

In beiden Fällen schafft OTR Abhilfe. Im Gegensatz zu GPG gibt es nicht nur einen Schlüssel mit dem Nachrichten entschlüsselt werden können, sondern es gibt eine Art Basis-Schlüssel aus dem ein neuer Schlüssel pro Gespräch generiert wird. Für den Fall, dass ein „Gesprächsschlüssel“ geknackt/geklaut wird, hat dies den Vorteil, dass nur das zu dem „Gesprächsschlüssel“ gehörige Gespräch entschlüsselt werden kann und nicht alle anderen, wie bei GPG.

Bei der Nutzung von OTR ist es wichtig, den Kommunikationspartner zu verifizieren. (Stichwort Pidgin Unverifizierte Unterhaltung).

Surfen

TOR

Tor (ehemals „The onion router“) ist ein Netzwerk zur Anonymisierung von Verbindungsdaten. Das bedeutet alle Daten, die du durch das Tor-Netzwerk schickst, werden willkürlich und verschlüsselt über drei Computer (sogenannte Nodes) zu ihrem Ziel geleitet. Dabei weiß der letzte Computer in der Kette (der sogenannte Exit-Node) nicht mehr, woher die Daten ursprünglich stammen. Somit erfährt das Ziel (z.B. eine Webseite) nicht, wer dessen Inhalte abruft. Um anonym im Internet surfen zu können, sollte man das Tor-Browser Bundle verwenden.

empfohlene Browser-Plugins

- HTTPS-Everywhere (verschlüsselt Verbindungen wenn möglich)
- PrivacyBadger (blockiert Dienste, welche eine Bewegungsprofil erstellen)
- AdblockEdge (Werbeblocker)

Passwörter

KeepassX / Passwortmanager

Bei der Verwendung von Passwörtern gilt zum Einem, dass ein Passwort aus einer Kombination von mindestens 12 Zeichen, Ziffern sowie Sonderzeichen bestehen sollte. Zum Anderen soll man jedes Passwort nur ein einziges Mal verwenden! Bei der Fülle von verschiedenen Passwörtern (Festplattenverschlüsselung , Email, Ebay, Bank ...) kann man sehr schnell den Überblick verlieren. Deswegen bietet sich die Nutzung eines Passwortmanagers an. Mit diesem ist es möglich, seine Passwörter in einer verschlüsselten Datenbank auf seinem Computer zu speichern und sich zum Beispiel Passwörter automatisch generieren zu lassen. Um die Passwortdatenbank zu öffnen benötigt man lediglich das dazugehörige „Master-Passwort“. Verwendet man solch einen Passwortmanager muss man sich lediglich ein Passwort merken. Bekannte Passwortmanager sind zum Beispiel keepass oder 1Password.

sicheres Arbeiten

Tails

Tails ist ein Akronym für „The Amnesic Incognito Live System“. Dieses ermöglicht es dem/der Benutzer*in mit Hilfe eine Live-USB-Sticks auf einem Computer anonym zu arbeiten und dabei die Privatsphäre zu wahren, da es keine Spuren auf dem Computer hinterlässt. In Tails sind verschiedene Tools zum Schutz der Privatsphäre integriert und standardmäßig aktiviert (z.B. Tor, GPG und viele mehr). Weiterhin ist es möglich, wichtige Informationen verschlüsselt auf dem selben USB-Stick abzulegen und bei der nächtsten Verwendung von Tails zu verwenden / bearbeiten. Erst kürzlich wurde in deutscher Guide zu Tails veröffentlicht in dem du alle Informationen zu Tails und den eingesetzten Anonymisierungswerkzeugen nachlesen kannst: https://capulcu.nadir.org/

sicheres Handy 1

Textsecure

TextSecure ist eine kostenlose Android App mit der man verschlüsselte Nachrichten austauschen kann. Die Nachrichten können sowohl Gruppen- oder Einzelnachrichten sein und aus Text oder Bildern bestehen. Die verschlüsselte Kommunikation kann sowohl als SMS, als auch über den Datenkanal des Telefons geschehen. Im Gegensatz zu der Vielzahl von anderen verschlüsselten Messenger-Apps ist Textsecure OpenSource. TextSecure wurde von OpenWhisperSystems entwickelt, welche auch die Apps Redphone/Signal zum verschlüsselten telefonieren kreiert haben. Sag es deinen Freun*innen: Weg von WhatsApp - TextSecure ist eine vollwertige und sichere Alternative.

Redphone / Signal

Redphone und Signal sind zwei kostenlose Open-Source Apps, die es auf dem jeweiligen Betriebssystem ermöglichen, verschlüsselte Telefonate zu führen. Dies ist plattformübergreifend sowohl mit anderen Redphone- als auch Signal-Nutzer*innen möglich. Die Telefonate werden über die Internetverbindung des Mobilgeräts aufgebaut und sind deswegen keine klassischen Anrufe via Telefonnetz, sondern sogenannte Voice-over-IP-Telefonate (VoIP).

sicheres Handy 2

Redphone / Signal

Redphone und Signal sind zwei kostenlose Open-Source Apps, die es auf dem jeweiligen Betriebssystem ermöglichen, verschlüsselte Telefonate zu führen. Dies ist plattformübergreifend sowohl mit anderen Redphone- als auch Signal-Nutzer*innen möglich. Die Telefonate werden über die Internetverbindung des Mobilgeräts aufgebaut und sind deswegen keine klassischen Anrufe via Telefonnetz, sondern sogenannte Voice-over-IP-Telefonate (VoIP).