5. Mit dem Chatten beginnen:
Damit man auf diesem Wege verschlüsselt chatten kann, muss selbstverständlich auch jeder andere Teilnehmer eine eigene ID mit Schlüssel erzeugt haben und OTR installiert haben. Man muss die ID des anderen wissen und als Kontakt (Buddy) bei Pidgin eintragen. Achte darauf, dass OTR aktiviert und der Chat als privat gekennzeichnet ist.

Eine ausführlichere Anleitung auf deutsch:
http://nureinhobby.org/invader/uncategorized/verschlusseltes-chatten-mit-pidgin-und-otr-unter-windows-fur-anfanger/

Und eine weitere hilfreiche Anleitung auf englisch:
http://tips.webdesign10.com/free-software/how-use-jabber

Der Blick nach vorne

Zwischenmenschliche Kommunikation muss möglich sein, ohne dass man Sorge haben muss, dass persönliche Gespräche und Unterhaltungen von Dritten mitverfolgt oder gar gespeichert oder ausgewertet werden.

Das verschlüsselte Chatten bietet uns die Möglichkeit, das in unseren Lebens- und Kommunikationsalltag umzusetzen. Zudem erlaubt das Chatten eine flotte Kommunikation, die Gruppenprozesse sehr viel einfacher und effektiver machen kann.

Wenn ihr Gefallen am verschlüsselten Chatten gefunden habt, dann tragt bitte den Gedanken und die Informationen weiter. Organisiert und unterstützt euch beim Austausch von Erfahrungen, teilt euer Wissen mit anderen.

Oder setzt einen eigenen Jabber-Server auf – das ist relativ unkompliziert und kann dazu beitragen, dass eine dezentrales und unabhängig aufgebautes Kommunikationsnetz fernab aller Konzern- oder Überwachungsinteressen entsteht.

Wichtige Hinweise - das Kleingedruckte zum Schluß

Es gibt keine 100%ige Sicherheit – nirgendwo. Verschlüsseltes Chatten mit OTR ist eine wirklich gute Sache. Aber wenn euer Rechner z.B. von einem Spionagetrojaner befallen ist, nützt hilft das im Extremfall nicht viel. Das sollte man wissen.

Neben Pidgin bieten auch andere Programme die OTR-Verschlüsselung und es gibt noch einige ganz andere Ansätze zum verchlüsselten Chatten, z.B. „Retroshare“. Schaut euch um, informiert euch!

Impressum
www.freiheitsfoo.de
CC-BY-NC-SA
Stand: 02/2013

Verschlüsselt und abstreitbar chatten

Worum geht es?

Kommunikation ist wichtig. Für Menschen, ihr Wohlbefinden und ihre Entwicklung und damit für das Zusammenleben von Menschen, für die Gesellschaft.

Die elektronisch geführte Kommunikation nimmt zu und schafft viele neue Chancen und Möglichkeiten des Austausches und des Engagements.

Gleichzeitig sind Behörden und Unternehmen immer stärker daran interessiert (und aktiv!), unser Kommunikationsverhalten zu erfassen, zu speichern und für ihre eigenen Zwecke auszuwerten.

Nur wer sich von der Sorge, ständig unter Beobachtung und Bewertung zu stehen, frei machen kann, hat auch eine Chance auf eine freie Entfaltung und Entwicklung.

Das Verschlüsseln von E-Mails und/oder Speichermedien sind einige wichtige Schritte auf diesem Weg.

Aber es gibt eine weitere, sehr interessante Möglichkeit, sich sehr unkompliziert und zudem verschlüsselt miteinander auszutauschen:

Chatten mit Verschlüsselung

(Verschlüsseltes) Chatten ist sehr viel schneller und unkomplizierter als verschlüsseltes Mailen, reicht für viele Zwecke aus und ermöglicht darüber hinaus diskussionshafte Gruppengespräche bis hin zum sicheren Austausch von Dateien und Verschlüsseln von Video-Konferenzen. Damit ist es für viele Menschen und Gruppen ein attraktives Werkzeug.

Was ist „chatten“ und wer ist „Pidgin“?

„Chatten“ kommt vom englischen „to chat“ und heisst in etwa so viel wie klönen, plaudern, quatschen, schwatzen, schnacken … Damit ist schon mal erklärt, wofür Chatten steht. ☺

Wenn man mit Hilfe des Internets chatten will, benötigt man eine entsprechende Software, die das ermöglicht und eine Infrastruktur im Internet, die dafür vorbereitet ist. Neben den seit längerem verbreiteten „IRC = Internet Relay Chat“ hat sich auch der so genannte „Webchat“ innerhalb von Internetbrowsern durchgesetzt. Eine dritte technische Möglichkeit stellt das **„Instant Messaging“** dar, und darum soll es hier gehen.

„Instant Messaging“ bedeutet, dass sich zwei oder mehr Menschen miteinander mittels Textblöcken unterhalten. Sie „chatten“ miteinander. Jeder Teilnehmer muss dazu eine Software installiert haben, die das ermöglicht. Zum Beispiel das freie Programm **„Pidgin“**, das es sowohl für Windows als auch für Linux gibt. (Für das Apple-Betriebssystem wäre „Adium“ eine Alternative zu Pidgin.)

Es haben sich sehr viele unterschiedliche Standards für die Übertragung der Daten entwickelt. Diese Standards bezeichnet man als **„Protokoll“** und diese Protokolle haben so seltsame Namen wie z.B. „ICQ“, „MSN“, „IRC“, „XMPP“ und noch viele mehr.

Das Programm Pidgin bietet den großen Vorteil, dass es eine sehr umfangreiche Anzahl von unterschiedlichen Protokollen bedienen kann.

Vor allem aber bietet Pidgin die Möglichkeit, das **XMPP-Protokoll** (bekannt von Google+, Facebook etc.!) und das darauf aufbauende Verschlüsselungsprotokoll namens **„OTR“** zu benutzen. Der Wechsel von vom unverschlüsselten zum verschlüsselten Chatten fällt damit besonders leicht. Alte Kontakte gehen nicht verloren.

Übrigens (zur Aufklärung):

Chatten mit dem XMPP-Protokoll wird häufig auch als „jabbern“ bezeichnet. „Jabber“ war das erste Programm, das es zum XMPP-chatten gab.

Sicher chatten mit OTR

Mit Hilfe eines Plugins (das ist so was wie eine App bzw. ein Add-On) kann man Pidgin zur Verwendung des „OTR-Protokolls“ befähigen. (Bei Adium für Apple-Rechner ist das sogar schon vorinstalliert.)

„OTR“ steht für „Off The Record Messaging“, was nicht mehr oder weniger bedeutet als eine vertrauliche, nicht für die Öffentlichkeit bestimmte Übermittlung von Nachrichten.

Kurz und gut – wer das OTR-Protokoll zum Chatten benutzt, der kann folgende Vorteile auskosten:

1. Verschlüsselung
Das verschlüsselte Chatten mit OTR erfolgt auf eine sehr sichere Art und Weise verschlüsselt, also für andere in aller Regel nicht mitlesbar.
Bedingung: Alle Chat-Teilnehmer müssen die Möglichkeit zum OTR-Protokoll installiert und aktiviert haben.

2. Authentizierung
OTR erlaubt die Authentifizierung des Gegenübers. Man kann sich dann also sehr sicher sein, mit wem man sich gerade unterhält.
Bedingung: Anfangs muss eine Authentifizierung zwischen Gesprächspartnern neu durchgeführt werden. Dafür bietet das OTR-Plugin eine automatisierte Unterstützung an.

3. Abstreitbarkeit
Die übermittelten Nachrichtenpakete sind ohne Signatur. Das bedeutet, dass die Nachrichten später, im Nachhinein zwar theoretisch durch Dritte gefälscht werden könnten, dass man aber als Betroffener die Urheberschaft dieser eventuell manipulierten Nachrichten u.U. rechtlich erfolgreich abstreiten kann.

4. Folgenlosigkeit
Selbst bei Verlust des Rechners oder des eigenen bei Pidgin gespeicherten Schlüssels können die zuvor geführten Unterhaltungen nicht wieder entschlüsselt werden. Das erleichterte eine unbefangene Kommunikation.

Wie geht das?

Hier ist eine einfache Anleitung, **hauptsächlich für Windows-Benutzer gedacht**, Linux-User dürften sich den Rest selber zusammenreimen können:

1. Pidgin herunterladen und installieren:
http://pidgin.im/download/

2. Das OTR-Plugin für Pidgin installieren:
http://www.cypherpunks.ca/otr/binaries/windows/pidgin-otr-4.0.0-1.exe

3. OTR aktivieren:
Im Menüpunkt Werkzeuge/Plugins bei dem Plugin „Off-the-record Messaging“ ein Häkchen setzen und die OTR-Verschlüsselungsmöglichkeit damit einschalten.

4. Ein Benutzerkonto anlegen:
Dazu unter Konten/Konten-verwalten/Hinzufügen als Protokoll XMPP wählen. Dann einen eigenen Benutzernamen oder Nicknamen ausdenken, z.B. „mustermensch“. Schließlich noch einen öffentlichen Jabber Server wählen, wie z.B. den vom Chaos Computer Club: jabber.ccc.de. (Also in diesem Fall „mustermensch“ bei „Benutzer“ und „jabber.ccc.de“ bei „Domain“ eingeben.) Ein eigenes, neues und gutes Passwort ausdenken und eintragen. Unter „Erweitert“ bei „Verbindungssicherheit“ „Verschlüsselung fordern“ einstellen.
Die damit erzeugte ID würde dann in diesem Fall „mustermensch@jabber.ccc.de“ lauten.