SICHERES CHATTEN

Viel Onlinekommunikation läuft über Chatprogramme beziehungsweise Instant Messaging (Sofortnachrichten) ab. Fast jede ComputerbenutzerIn hat heutzutage zumindest einen Account bei einem Onlinechat-Dienst. Die Urgesteine der Internetgeneration schwören auf IRC, die Älteren unter uns werden wahrscheinlich noch ICQ oder MSN zum Chatten verwenden, in den letzten Jahren hat sich die Kommunikation per Skype oder Facebook stark durchgesetzt. Die fünf großen proprietären Instant Messenger sind AIM (AOL Instant Messenger), ICQ, Windows Live Messenger, Yahoo Messenger und Skype. Offene Ansätze sind zum Beispiel Jabber, IRC oder SILC.
Wichtig ist es diesbezüglich, sich nicht in die Fänge einer Firma zu begeben und auf sichere Übertragung der Kommunikationsinhalte zu achten, um den Ermittlungsbehörden das Ausforschen derer nicht zu einfach zu machen.

Protokoll versus Programm

Gerade in den letzten zehn Jahren ist die Welt der Chatprogramme sehr unübersichtlich geworden. Im normalen Sprachgebrauch werden die Programmnamen und die Protokollnamen der Chatprogramme oft vermischt. Das Protokoll ist so etwas wie die Sprache, in der die einzelnen Chatprogramme miteinander kommunizieren und Nachrichten austauschen. Z.B. verwenden die Programme ICQ und AIM das Protokoll OSCAR um die Nachrichten auszutauschen. Da das Programm ICQ nur für Windows zur Verfügung stand, haben sich findige ProgrammiererInnen genauer angesehen, wie die Programme miteinander sprechen und haben dann selber Programme geschrieben, mit denen es möglich ist, an dem ICQ-Netzwerk teilzunehmen. Jedoch wurden solche Ansätze immer wieder durch Änderung des Protokolls stark behindert. Im Laufe der Zeit waren die ProgrammiererInnen dann so angepisst, dass sie einfach eigene freie (nicht kommerzielle, offene) Instant Messaging Protokolle erfunden haben. Das momentan am meisten verbreitetste davon ist Jabber (auch als XMPP bekannt). Im Weiteren ging die Entwicklung dahin, dass viele Clients (also die Programme zum Chatten) nicht nur ein Protokoll sprechen konnten sondern viele (z.B. die Programme Pidgin und Miranda).

Die Nachteile von proprietären Netzwerken

In einem Grossteil der Fälle ist die Nutzung eines proprietären Netzwerks an die Nutzung eines proprietären Programms gebunden. Auf die Nachteile von proprietärer Software muss hier nicht näher eingegangen werden. Weiters steht bei AIM zum Beispiel in den Nutzungsbedingungen, dass die Teilnahme mit alternativen Clients untersagt ist. Ein Nachteil an ICQ ist, dass die dahinterstehende Firma das Copyright an allen Daten, die über das Netzwerk versendet werden, bekommt. Ähnliche Klauseln gibt es auch in den AGBs von AIM und MSN. Also wenn ihr ein Gedicht schreibt und das jemandem über ICQ zuschickt, gehört das Gedicht dann der Firma hinter ICQ.
Die Firma Skype hat zugesagt, jederzeit mit den Ermittlungsbehörden zusammenarbeiten, sofern es Anfragen gibt. Im August 2010 wurde bekannt, dass die deutschen Behörden Skype schon abhören können und Abhörprotokolle schon vor Gericht verwendet werden!
Kurz gesagt legt ihr bei der Verwendung von proprietären AnbieterInnen eure gesamte Chat-Kommunikation in die Hände einer Firma.
Aus diesen Gründen liegt es nahe, auf offene Systeme, die nicht an eine AnbieterIn gebunden sind, wie zum Beispiel IRC oder Jabber, zurückzugreifen.

IRC

Beim Internet Relay Chat sucht ihr euch einen Nickname und verbindet euch mit einem IRC Programm zu einem Server. Dieser Server ist entweder alleinstehend oder er ist Teil eines IRC-Netzwerks. Auf dem Server oder in dem Netzwerk gibt es dann die verschiedensten Channels (Chaträume). Ihr könnt dann einen der Channels 'betreten' und gleich mit den anderen Personen in dem Channel anfangen zu sprechen. Wichtig ist, dass ihr, falls das möglich ist, über eine verschlüsselte Verbindung auf den Server zugreift, damit nicht mitgelauscht werden kann, was ihr an den Server schickt. Ihr müsst euch dazu nicht auf dem Server registrieren, es ist aber möglich. Das ist dann sinnvoll, wenn ihr wiedererkannt werden wollt da es sonst kein Möglichkeit gibt, zu überprüfen ob hinter eurem Pseudonym noch immer diesselbe Person steckt wie vor einer Woche. In den Channels gibt es dann meistens ModeratorInnen, die verschiedene Aufgaben übernehmen, wie zum Beispiel das Herauswerfen von Trollen. Es ist auch möglich über private Nachrichten mit nur einer Person zu chatten. Dies funktioniert aber nur mit Leuten die im gleichen Netzwerk angemeldet sind.
Es gibt bei IRC ziemlich wenig Anonymität, da alle anderen UserInnen des Netzwerkes eure IP-Adresse herausfinden können. In dem Netzwerk von Indymedia (irc.indymedia.org) ist es möglich, nach Registrierung, die Server AdminAs zu bitten, eure IP-Adresse für andere UserInnen zu verstecken.
Programme für die Teilnahme an IRC Channels sind zum Beispiel Empathy (Linux), Pidgin (Windows, Linux, OS X), XChat (Linux/Windows), Chatzilla (Firefox Erweiterung).

SILC

SILC steht für Secure Internet Live Conferencing (Sichere Konferenz via Internet, in Echtzeit) und wird so wie IRC vor allem für Chaträume verwendet. SILC hat eine oberflächliche Ähnlichkeit zu IRC, ist aber intern vollkommen anders aufgebaut. Ein Unterschied zu den meisten anderen Chatprotokollen ist, dass SILC sichere Kommunikation über unsichere Netze ermöglicht, da es die Möglichkeit bietet Nachrichten auf dem gesamten Übertragungsweg verschlüsselt zu lassen.
Die Kollektive riseup, immerda und so36.net bieten gemeinsam ein SILC Netzwerk an. Als Client empfiehlt sich hier wieder Pidgin.

Jabber

Jabber ist im Gegensatz zu IRC ein typisches Instant Messaging Protokoll. Es gibt dabei sowohl den Chat von Person zu Person als auch Channels, die bei Jabber als Conference Room (Konferenzraum) bezeichnet werden. Auch bei Jabber gibt es verschiedene Server oder Netzwerke, jedoch können die BenutzerInnen von diesen alle miteinander kommunizieren (O.k., nicht überall- Facebook verwendet für seine Chatanwendung auch Jabber, erlaubt aber die Kommunikation mit anderen Servern nicht).
Für die Verwendung von Jabber müsst ihr euch zuerst mit eurem Jabber Client auf dem Server einen Nickname registrieren. Bevor ihr euch irgendeinen Server raussucht, informiert euch am besten, wer ihn wie betreibt (z.B. wird der Jabber-Server jabber.org mit proprietärer Software betrieben und ist deswegen nicht zu empfehlen).
Ihr verbindet euch dann mit eurem Client immer zu diesem Server. Auch hier ist es wichtig, dass ihr darauf achtet, dass die Verbindung zum Server verschlüsselt ist. Dann könnt ihr im Jabber Programm Verbindung zu anderen UserInnen aufnehmen, indem ihr sie zu eurer Buddy-Liste (sozusagen eine FreundInnen Liste) hinzufügt. Wenn ihr einen Konferenzraum betreten wollt, dann müsst ihr diesen auch zu eurer Buddy-Liste hinzufügen.
Es gibt bei Jabber auch die Möglichkeit von (Video)-Telefonie. Dies wird mittels einer Erweiterung des Protokolls namens Jingle gelöst, die Peer-To-Peer Verbindungen ermöglicht. Das heisst, dass sich eure Jabber Programme direkt miteinander verbinden und sich die Daten direkt schicken, ohne Umweg über einen Server.
Programme für die Teilnahme an Jabber sind zum Beispiel Empathy (Linux), Pidgin (Windows, Linux, OS X), Psi (Windows, Linux, OS X).

Verschlüsselung von Nachrichten: OTR

Wenn wir bis jetzt erwähnt haben, dass ihr bei der Verbindung zum Server auf Verschlüsselung achten sollt, dann ist nur die Verbindung verschlüsselt, jedoch nicht die Nachrichten, die über diese Verbindung gehen. Möglichweise übertragen die Server die Nachrichten untereinander unverschlüsselt und es kann auf dazwischen liegenden Punkten mitgelauscht werden oder auf den Servern selbst kann mitgelauscht werden. Oder es sitzt jemensch am anderen Ende, der/die gar nicht die Person ist, mit der ihr chatten wollt. Um dieses Problem aus dem Weg zu schaffen, wurde Off The Record Messaging (vertrauliche Nachrichtenvermittlung) entwickelt. OTR verwendet im Gegensatz zur Email-Verschlüsselung mit GPG ein symmetrisches Verschlüsselungsverfahren- hier wird nur ein Schlüssel erzeugt, der sowohl für Ver- als auch für Entschlüsselung von Nachrichten verwendet wird.
Zusätzlich werden die Inhalte noch mit einem zeitlich begrenzten Schlüssel (Session-Key) verschlüsselt. Das heisst, dass jemensch, der die verschlüsselten Nachrichten in die Hand bekommt (zum Beispiel durch mitlauschen), diese im Nachhinein nicht entschlüsseln kann, weil der passende Schlüssel abgelaufen ist. Wichtig ist hierbei natürlich, dass die Chatprogramme selber nicht die Inhalte mitloggen- das muss händisch deaktiviert werden! Weiters gibt es das Prinzip der Abstreitbarkeit- damit ist gemeint, dass mit dem verschlüsselten Datenstrom nicht nachgewiesen werden kann, welche Kommunikations-partnerInnen diesen verursacht haben.
Im Gegensatz zu Email, wo es öffentliche Schlüssel gibt, die am besten persönlich ausgetauscht werden, wird bei OTR das Problem des Erstkontaktes (also ob die Person am anderen Ende wirklich die ist, mit der ihr reden wollt) mittels Shared Secret, also einem gemeinsamen Geheimnis, gelöst. Dabei wird beiden KommunikationspartnerInnen eine Frage gestellt, die sie beantworten müssen. Die Antwort haben sich beide vorher ausgemacht. Es ist natürlich auch möglich, den Schlüssel der Kommunikationspartnerin persönlich zu überprüfen. Am Besten ist es natürlich, beide Möglichkeiten gemeinsam zu nutzen.
Zu beachten ist auch, dass Dateien, die über die Instant Messaging Netzwerke übertragen werden, nicht(!) von OTR verschlüsselt werden, diese sollten händisch verschlüsselt werden (zum Beispiel mit GPG)!
OTR gibt gibt es als Plugin für die verschiedensten Chatprogramme und es ist unabhängig vom Protokoll. Das heisst, dass es sowohl über IRC als auch über Jabber verwendbar ist. Leider gibt es noch nicht soviele Clients, die OTR unterstützen, jedoch gibt es für Pidgin, das ja IRC und Jabber (u.v.m.) sprechen kann, ein Plugin von den OTR ErfinderInnen.

Indymedia IRC Server
irc.indymedia.org
https://chat.indymedia.org
SILC Netzwerk
https://www.so36.net/dienste/silc-network
Jabber Server bei linken Kollektiven
https://immerda.ch/index.php/Jabber
https://so36.net/howtos/jabber-account-mit-pidgin
https://www.autistici.org/en/services/instantmessaging/index.html
OTR Website
http://www.cypherpunks.ca/otr

tear the system down - bit. by. bit. mailto:bitbybit@riseup.net
technologie in linksradikalen kontexten https://we.riseup.net/bitbybit