Messenger

Um verschlüsselt zu kommunizieren, eignen sich neben verschlüsselten Mails einige Messenger. Vorteilhaft gegenüber Mails sind (gute) Messenger, weil bei ihnen Verschlüsselung und sichere Kommunikation von vornherein mit gedacht wurden. Dafür sind sie, vor allem die besseren, aber weniger verbreitet.

Kriterien, was einen guten Messenger auszeichnet, finden sich z.B. bei Digitalcourage. Für Aktivist*innen ist (je nach Threat Model) vor allem eine möglichst sichere, Daten-sparsame und anonyme Kommunikation wichtig.

Hierfür soll auf zwei in Aktivismuskreisen recht weit verbreitete Messenger, die mit Einschränkungen zu empfehlen sind, eingegangen werden: Signal und Matrix.

Signal

Signal wurde von dem Anarchisten Moxie Marlinspike entwickelt und ist eine der bekanntesten Alternativen zum Monopolisten WhatsApp.

Vorteile von Signal

- **Einfache Nutzung**: Signal ist simpel zu installieren und "funktioniert einfach". Mensch kann nicht viel falsch machen, was die Sicherheit gefährden würde.
- **Weite Verbreitung**: 2022 hatte Signal 40 Millionen aktive Nutzer*innen. Damit liegt es zwar noch immer weit hinter den 2 Milliarden Nutzer*innen von WhatsApp, ist aber dennoch weit verbreitet.
- **Sichere Verschlüsselung**: Signal hat ein eigens Kommunikationsprotokoll, das quell-offen ist und regelmäßig geprüft wird. Einige andere Messenger, wie WhatsApp haben das Protokoll ebenfalls übernommen, sodass sich das Protokoll durch die Nutzung von Milliarden von Menschen bewährt. Die Kommunikation in Signal ist demnach sicher Ende-zu-Ende-verschlüsselt.
- **Daten-Sparsamkeit**: Signal speichert möglichst wenig über die Nutzer*innen und kann demnach auch nur wenige Informationen preisgeben. Die einzigen Daten, die Signal in vergangenen Gerichtsprozessen raus *konnte*, waren das Erstellungsdatum des Accounts und das Datum, als der Account zuletzt genutzt wurde.

- **Möglichkeit der automatischen Löschung**: Chats können so eingestellt werden, dass sich die Nachrichten automatisch nach einer bestimmten Zeit löschen. So sind sie selbst dann sicher, wenn Cops (nach dieser Zeit) Zugriff auf das Gerät erhalten.

Nachteile von Signal

- **Anonymität**: Signal wurde nicht entwickelt um anonym zu sein, sondern um sichere Verschlüsselung anzubieten. Stand heute (Januar 2024) ist eine Telefonnummer notwendig, um sich zu registrieren; diese muss (rein rechtlich) auf eine real existierende Person registriert sein. Die Telefonnummer ist sichtbar für alle, mit denen mensch kommuniziert. Die konkrete Gefahr ist hier, dass entweder ein Cop in einem sensiblen Chat ist und mensch so identifiziert wird, oder dass ein Handy mit Zugriff auf sensible Chats konfisziert wird.
- **Sitz in den USA**: Die Signal Foundation hat ihren Sitz in den USA und kann demnach gezwungen werden, Daten an Geheimdienste weiter zu geben.
- **Zentralität**: Signal läuft nur über die eigene Infrastruktur (die bei Amazon, Microsoft, Google und Cloudflare liegt) und lässt sich nicht selber hosten. Somit muss mensch Signal ein Stück weit vertrauen, dass sie ihren Job gut machen. Außerdem gibt es somit eine zentrale Stelle, die angegriffen werden kann.

Matrix

Matrix ist ein Kommunikationsprotokoll (ähnlich wie Mail, bzw. genauer so was wie IMAP, eines ist).

Für dieses Protokoll gibt es diverse Clients, der bekannteste ist Element. Vor allem in letzter Zeit findet Matrix mehr Verbreitung in Aktivismus- und Hackerkreisen.

Funktionsweise

Der wichtigste Unterschied von Matrix im Vergleich zu anderen Messengern, wie z.B. Signal, ist die Dezentralität, bzw. *Föderation*. Ähnlich wie bei Mails gibt es viele verschiedene Server ("*Homeserver*") (wie z.B. *matrix.org* oder *matrix.systemli.org*). Kommuniziert ein Aktivisti mit einem Matrix-Account bei matrix.org mit einem Aktivisti mit einem Matrix-Account bei matrix.systemli.org, so müssen die (verschlüsselten) Nachrichten zwischen den beiden Servern synchronisiert werden.

Matrix Föderation Funktionsweise

Vorteile von Matrix

- **Sichere Verschlüsselung**: Matrix nutzt eine eigene Implementation des Signal-Protokolls. Es hat Nachteile im Vergleich zum Signal-Protokoll, ist aber dennoch ähnlich sicher.
- **Dezentralität**: Matrix ist föderiert und damit dezentral. Es gibt viele verschiedene Server, die miteinander kommunizieren; somit gibt es viele Stellen, die angegriffen werden müssten, um ganz Matrix lahm zu legen.
- **Anonymität**: Bei einigen Servern werden keine persönlichen Informationen zur Erstellung eines Accounts benötigt. Somit ist es prinzipiell möglich, Matrix anonym zu nutzen.
- **Offenheit**: Der Quelltext von Matrix, sowie von Element ist quelloffen und kann (und wird) regelmäßig überprüft.

Nachteile von Matrix

- **Komplizierte Nutzung**: Zuweilen ist es kompliziert, Matrix zu nutzen. Das Prinzip der Föderiertheit ist unintuitiv, es gibt viele sehr verschiedene Clients und vieles funktioniert nicht einfach.
- **Noch nicht weit verbreitet**: Menschen müssen häufig erst mal dazu überredet werden, sich einen Matrix-Account einzurichten.
- **Mangelnde Daten-Sparsamkeit**: Weil Matrix föderiert ist, müssen alle Daten auf allen föderierten Servern synchronisiert werden. Das bedeutet auch, dass es praktisch unmöglich ist, Daten wieder zu löschen. Auf allen Servern werden standardmäßig für immer die Matrix ID persönliche Informationen, Nutzungsdaten, IP-Adressen, Geräteinformationen, andere Server mit denen kommuniziert wird und Raum-IDs gespeichert. (Die Quelle bezieht sich auf eine ältere Matrix-Version. Inwiefern die standardmäßig gespeicherte Datenmenge und das Löschverhalten auf aktuelle Versionen übertragbar sind, ist unklar.)

Resümee

Für den aktivistischen Alltag, in dem mensch nicht anonym sein möchte, eignet sich Signal sehr gut. Insbesondere im Vergleich zu kommerziellen Alternativen ist es Privatsphäre-freundlich und sicher. Sollte aber doch mal Anonymität (und gleichzeitig eine sichere Verschlüsselung) in der digitalen Kommunikation wichtig sein, eignet sich Matrix besser. Hier sollte dann aber darauf geachtet werden, dass keine persönlichen Informationen (wie die IP-Adresse) preis gegeben werden, da diese auf den Servern liegen bleiben.

Version #2
Erstellt: 14 Januar 2025 18:53:21 von ESC-IT Migration Bot
Zuletzt aktualisiert: 27 Januar 2025 21:28:18 von ESC-IT Migration Bot