Messenger

Cryptoparty 30.07.18

Was sind (Instant) Messenger

- Echtzeitkommunkation, meist via Internet
- Sehr einfach in der Nutzung, besonders auf Smartphones
- Bieten mehr Funktionalität als nur Austausch von Nachrichten
    - Teilen von Dateien, Standort, Kontakten

Messenger

- SMS-Ersatz (WhatsApp, Signal, …)
  - Direkt- und Gruppenchats, Telefonie
  - Nutzen oft Telefonnummer zur Identifizierung
    - Kein “klassisches” Benutzerkonto mit Passwort benötigt
    - Adressbuch des Telefons kann genutzt werden
- Raum / Channel-basiert (Slack, Matrix, Discord, …)
  - Räume und Gruppenchats
  - Weit verbreitet in Communities und Firmen
  - Nutzen “klassische” Benutzerkonten

Messenger

- Zentralisierte Systeme (WhatsApp & Co):
  - Ein zentraler Diensteanbieter betreibt Infrastruktur und Apps
  - Auswahl des Dienstes bestimmt erreichbaren Personenkreis
- Dezentrale, offene Systeme (Jabber/XMPP, Matrix)
  - App-Entwickler, Dienstanbieter und Protokoll-Standardisierer sind unterschiedliche Personen
  - App und Anbieter frei wählbar
  - Meist Open Source

Risiken zentralisierter Messenger

Der Dienstanbieter sieht:

- Alle Metadaten
- Telefonbücher aller Nutzer
  - Weiß wer wen kennt
- Alle Nachrichten (wenn nicht Ende-zu-Ende verschlüsselt wird)
- Alle Nutzerprofile (Foto, Name, Status, etc.)

WhatsApp

- Open source: nein
- Ende-zu-ende: ja (Signal Protokoll)
- Desktop: jain (via Smartphone)
- Speichert Adressbuch nach Upload
- Fraghafte Verbindung zu Facebook
- Tipp: Account -> Security -> Show security notifications

Facebook Messenger

- Open source: nein
- Ende-zu-ende: jain (Secret Chat über Signal Protokoll)
- Eng verbunden mit Facebook-Account
- Kann ohne Facebook-Account genutzt werden (Telefonnummer)
- Lädt laufend Adressbuch und Anrufliste hoch (kann deaktiviert werden)
    - Tipp: Hochladen und Verwalten deiner Kontakte

Telegram

- Open source: ja (Client)
- Ende-zu-ende: jain (MTProto + Secret Chat)
- Desktop: ja
- Speichert Adressbuch nach Upload
- Unsichere Standardeinstellungen

Threema

- Open source: nein (aber: Audits und Dokumentation)
- Ende-zu-ende: ja
- Desktop: jain (via Smartphone)
- Anonym: Telefonnummer oder E-Mail optional (Threema-ID)
  - Kontaktaustausch via QR-Code
- Upload des Adressbuchs optional
- Nicht kostenlos: 2,99€ Android / 3,49€ iOS
  - Klares Geschäftsmodell
  - Kommunikationspartner müssen App kaufen

Signal

- Open source: ja
- Ende-zu-ende: ja (Signal Protokoll)
- Desktop: ja
- Betreiber: Open Whisper Systems (Spendenfinanziert)
- Verschlüsselte Backups, Adressbuch optional
- Aktiv datensparsam (z.B. Private Contact Discovery Service)
- Von Experten empfohlen (Snowden, Bruce Schneier)
- “Signal does not sell, rent or monetize your personal data or content in any way – ever” - Signal ToS

Android-Tipps

- Zugriff auf Adressbuch verweigern (ab Android 6)
  - Senkt den Komfort, da oft keine Namen oder Fotos angezeigt werden
- Einige Messenger sind auch ohne Google Play nutzbar:
  - WhatsApp
  - Signal
  - Riot (Matrix)