Messenger – weiterführende Informationen

Eine Ausarbeitung von
Antje Hänzelmann (MiB)
und
Michael Georg Schmidt (ITS)
TH Lübeck

Version 1.0 Stand 16. Dezember 2020

Feedback
feedback-ah-mgs@protonmail.ch

Kontakt per Threema

Antje Hänzelmann Z2DVRRCY
Michael Georg Schmidt WYH86UFA

Präambel

Dieses Paper erhebt keinen Anspruch auf Vollständigkeit, sondern enthält lediglich Informationen, die den Autoren besonders wichtig erschienen. Es ist als Orientierung bei der Vielfalt an Messengern gedacht.

Ebenso sind Irrtümer möglich und es wird für die Richtigkeit der Angaben keine Verantwortung übernommen.

Inhaltsverzeichnis

1. Discord

Discord Support (Zum Thema Server Encoding – Server Verschlüsselung, 2020-14-12, https://support.discord.com/hc/en-us/community/posts/360043672952-Server-Encoding-Server-Verschl%C3%Bcsselung)

Datenschutzerklärung (Discord, Datenschutzerklärung, 2020-14-12, https://discord.com/privacy)

Anonyme Nutzung: Nein und Ende-zu-Ende -Verschlüsselung:
Eine Verschlüsselung der Nachrichten ist laut Discord in naher Zukunft nicht vorgesehen. Ein Argument des Supports war diesbezüglich, dass bei einer „Ende – zu-Ende -Verschlüsselung“ keine Daten, zum Beispiel Nachrichten, auf dem Server gespeichert werden könnten.
Weiterhin wurde argumentiert, dass dies bestimmte Features aushebeln würde und wer Wert auf volle Sicherheit lege, bei Discord nicht richtig sei.
Umgang mit Metadaten:
In der Datenschutzerklärung wird allgemein erläutert, dass Informationen, die freiwillig von den Nutzern zur Verfügung gestellt werden, gesammelt werden. Dazu gehören unter anderem der Nutzername, die E-Mailadresse, sowie alle Nachrichten, Bilder und alle weiteren Inhalte, die der Nutzer über die bereitgestellte Chat-Funktion versendet.
Discord ist ebenfalls dazu berechtigt, IP-Adresse, Geräte-ID und weitere Nutzeraktivitäten innerhalb der Dienste zu sammeln und in einer Datenbank abzuspeichern.
Weiter werden auf dieser Informationsgrundlage demografische Daten, Interessen und Verhaltensweisen der Nutzer untersucht und bei Bedarf mit den Geschäftspartnern von Discord geteilt.
Die Entwickler haben Zugriff auf Nachrichten- und Voice-Metadaten. Diese werden dazu verwendet, um Funktionalitäten innerhalb der Anwendung und Dienste zu gewährleisten.
Die personenbezogenen Daten werden laut der Datenschutzerklärung solange gespeichert, wie diese Zweck erfüllend sind. Daten können gelöscht, geändert oder anonymisiert werden. Sie können ebenfalls als Kopie zur Datensicherung für weitere Zeit gespeichert werden.
Discord bietet dem Nutzer die Möglichkeit an, auf die gespeicherten Daten zuzugreifen. Unter „Einstellungen“ gibt es eine Schaltfläche zum Herunterladen der Daten. Discord stellt einen Link zur Verfügung, dieser muss innerhalb von 30 Tagen verwendet werden.
In den Profileinstellungen könnten bestimmte E-Maildienste und Cookies unter „weitere Informationen“ deaktiviert werden.
Eine Korrektur, Aktualisierung oder Löschung der Daten kann verlangt werden. Auch kann Einspruch gegen die Verwendung und Weitergabe personenbezogener Daten erhoben werden, um eine Einschränkung der Verarbeitung zu verlangen. Dies gilt nicht rückwirkend und beeinträchtigt nicht die Befugnis von Discord, die Daten rechtmäßig zu verarbeiten.
Open Source/Closed Source:
Discord hat seinen Quellcode nicht veröffentlicht
Standort des Anbieters:
USA/Kalifornien
Kosten:
Discord stellt seine Dienste kostenlos zur Verfügung.

2. Element

- Datenschutzerklärung (TH Lübeck, Datenschutzerklärung für den Chat-Dienst der Technischen Hochschule Lübeck, 2020-14-12, https://chat.stud.th-luebeck.de/daterkl.html)
- Nutzungsbedingungen (TH Lübeck, Nutzungsbedingungen für den Chat-Dienst Technischen Hochschule Lübeck („THL-Chat“), 2020-14-12, https://chat.stud.th-luebeck.de/nutzbed.html)

Erläuterung
Die Datenschutzerklärung und die Nutzungsbedingungen sind so formuliert, dass sie aus Sicht eines Datenschützers inakzeptabel sind.
Auf Grund der Erklärung des IT-Supports der THL ist jedoch zu sagen, dass der Umgang mit den Nutzerdaten sorgfältig und zurückhaltend erfolgt. Die veröffentlichten Erklärungen sollten gern um die Erläuterungen des IT-Supports ergänzt werden.

Im Folgenden finden Sie diese Erläuterungen (Francsi, J., IT-Support THL, 2020-10-12):

Zugangsverwaltung: Vor- & Nachname(n), Mailadresse, Matrix-ID, Anzeigename sind Teil Ihres THL-IT-Kontos auf unseren Zentralen LDAP Servern und folgen somit den bereits genannten Löschfristen

Authentifizierung: Nutzername und Passwort müssen getrennt voneinander betrachtet werden. Die Anmeldung erfolgt über unsere LDAP Server. Der Benutzername taucht in den Logdateien auf (s.u.). Das Passwort wird auf den Matrix Servern nicht gespeichert.

Benutzerinhalte: Dies sind alle Daten, welche der Nutzer in das System eingibt (Ende-zu-Ende-verschlüsselung ist Standard). Die verschlüsselten Texte und Anhänge verbleiben nach dem Absenden 30 Tage auf unseren Servern und sind nur für die Teilnehmer einer Unterhaltung abrufbar. Die Teilnehmer können keine Nachrichten einsehen, welche vor ihrem Beitritt zu einer Unterhaltung gesendet wurden.

Geräteidentifikation (IP-Adressen mit Zeitstempel und Gerätename; verwendete Art des Endgerätes (Mobil / Desktop), Betriebssystem): Wir heben Logs auf den Servern zur Fehleranalyse und Gefahrenabwehr für 7 Tage auf. Zusätzlich sind die Gerätedaten Teil Ihres Matrix Profils und für die Kommunikation mit den von Ihnen verwendeten Clients notwendig.

Audio-/Video-Telefonie (IP-Adressen, AV-Daten): Die Server Routen die Gespräche in Echtzeit. Es findet keine Aufzeichnung auf unseren Servern statt.

Benachrichtigungen (Mail): Diese funktionieren derzeit nur teilweise (im Client, keine Mail). Benachrichtigungen wie z.B. Raumeinladungen verfallen nach 14 Tagen.

Eigenschaften

- E2EE auf Basis des „Matrix Protocol“ (Open Source) (The Matrix.org Foundation, An open network for secure, decentralized communication, matrix, 2020-14-12, https://matrix.org/)
  - gilt für die gesamte Kommunikation
- Kein Tracking
- Keine Werbung
- Kostenlos
- Gruppen-Chat
- Desktop App (Browser)
- Hohes Maß an Vertraulichkeit, da auf Servern der TH Lübeck

3. Messenger (Facebook)

Datenschutzerklärung (Facebook, Datenschutzerklärung, 2020-14-12, https://www.facebook.com/policy.php)

Anonyme Nutzung und Ende-zu-Ende -Verschlüsselung:
Laut Facebook ja, der Facebook Messenger bietet eine Möglichkeit an, Chats zu verschlüsseln. Dazu geht man auf einen seiner Kontakte, rechts oben auf den Infobutton und wählt die Option „geheime Unterhaltung aufrufen“. Ist die geheime Unterhaltung aktiviert, wird der Infobutton schwarz angezeigt.
Auch ein Selbstlöschmodus kann über den Infobutton durch einen Schieber aktiviert werden, das Chatfenster wird dann in schwarz angezeigt.
Gruppenchats und Videocalls werden nicht verschlüsselt.

Umgang mit Metadaten:
Inhalte, Kommunikationen und sonstige Informationen, die der Nutzer bereitstellt, werden erfasst, wenn dieser Facebook Produkte nutzt. Dazu gehört ebenfalls die Registrierung, für ein Konto, Erstellen oder Teilen von Inhalten, Nachrichtenaustausch und das Kommunizieren mit anderen. Dies kann die vom Nutzer bereitgestellten Informationen beinhalten, sowie Metadaten, wie den Aufnahmestandort eines Fotos oder das Erstellungsdatum einer Datei. Weiter werden Informationen über Personen, Seiten, Konten und Gruppen erfasst, mit denen der Nutzer verbunden ist. Es werden Kontaktinformationen gesammelt, wenn diese von einem Gerät hochgeladen, synchronisiert oder importiert werden (Adressbuch, Anrufprotokoll oder SMS -Protokollhistorie). Auch werden Zahlungsinformationen, wie Kreditkarten- oder Debitkarten Nummer oder sonstige Konto- und Authentifizierungsinformationen, sowie Abrechnungs- und Versandinformationen erfasst, sowie Kontaktangaben.
Geräteinformationen, wie zum Beispiel die Geräte -ID, Gerätesignale, Daten aus den Geräteeinstellungen (GPS-Standort, Kamera oder Fotos) werden gesammelt.
Unabhängig von dem Besitz eines Facebook Kontos können Werbetreibende und App-Entwickler Informationen über Aktivitäten, die außerhalb von Facebook stattfinden an Facebook senden, wie Geräteinformationen, besuchte Webseiten, getätigte Käufe, Werbung, genutzte Dienste, wenn diese Facebook Business Tools verwenden (Facebook-Pixel, Gefällt mir -Button).
Außerdem erhält Facebook von seinen Partnern Informationen über Online- und Offlinekäufe. Facebook verlangt von jedem Partner, dass dieser die gesetzlichen Rechte besitzt, Nutzerdaten zu erfassen, zu verwenden und zu teilen, bevor dieser Facebook die Daten zur Verfügung stellt.
Es wird zurzeit an einem eingeschränkten Datenzugriff für Entwickler gearbeitet. Zum Beispiel wird der Zugriff auf Facebook- und Instagramdaten aufgehoben, wenn die App drei Monate nicht genutzt worden ist.
Eine Übertragung von Nutzerinformationen an neue Eigentümer von Facebookanteilen ist möglich. Weiter schreibt Facebook, dass Nutzerdaten nicht direkt an Drittpartner verkauft werden.
Facebook ermöglicht dem Nutzer Auskunft, Berichtigung, Übertragbarkeit und Löschung seiner Daten. Auch kann Widerspruch gegen bestimmte Verarbeitung der Nutzerdaten eingelegt werden.
Facebook speichert die Daten, bis diese nicht mehr benötigt werden oder das Konto gelöscht wird. Dabei handelt es sich um eine Einzelfallbestimmung und hängt von der Art der Daten ab, wie diese erfasst und verarbeitet werden und den relevanten rechtlichen oder betrieblichen Speicherbedürfnissen.
Vor einer Änderung der Datenschutzbestimmung wird der Nutzer von Facebook informiert.
Open Source/Closed Source:
Facebook hat seinen Quellcode nicht veröffentlicht
Standort des Anbieters: USA/Kalifornien
Kosten: Facebook stellt seine Dienste kostenlos zur Verfügung.

4. Signal

- Terms of Service (Signal.org, 2018-25-05, Signal Terms & Privacy Policy, Terms of Service, 2020-14-12, https://signal.org/legal/#terms-of-service)
- Privacy Policy (Signal.org, 2018-25-05, Signal Terms & Privacy Policy, Privacy Policy, 2020-14-12, https://signal.org/legal/#privacy-policy)
- Daten die Signal speichert
  - Zeitpunkt der Registrierung
  - Zeitpunkt des letzten Kontakts zu Signal
  - „Additional technical information is stored on our servers, including randomly generated authentication tokens, keys, push tokens, and other material that is necessary to establish calls and transmit messages. Signal limits this additional technical information to the minimum required to operate the Services“ (Signal.org, 2018-25-05, Information you provide – Messages. signal.org, 2020-14-12, https://signal.org/legal/).
  - Kontakdaten (optional)
    „**Contacts.** Signal can optionally discover which contacts in your address book are Signal users, using a service designed to protect the privacy of your contacts. Information from the contacts on your device may be cryptographically hashed and transmitted to the server in order to determine which of your contacts are registered.“ (Signal.org, 2018-25-05, Information you provide – Contacts, signal.org, 2020-14-12, https://signal.org/legal/)
- Informationen die Signal teilt
  - „**Third Parties.** We work with third parties to provide some of our Services. For example, our Third-Party Providers send a verification code to your phone number when you register for our Services. These providers are bound by their Privacy Policies to safeguard that information. If you use other Third-Party Services like YouTube, Spotify, Giphy, etc. in connection with our Services, their Terms and Privacy Policies govern your use of those services.“ (Signal.org, 2018-25-05, Information we may share – Third Parties / Other instances where Signal may need to share your data, signal.org, 2020-14-12, https://signal.org/legal/)
  - „**Other instances where Signal may need to share your data**
    - To meet any applicable law, regulation, legal process or enforceable governmental request.
    - To enforce applicable Terms, including investigation of potential violations.
    - To detect, prevent, or otherwise address fraud, security, or technical issues.
    - To protect against harm to the rights, property, or safety of Signal, our users, or the public as required or permitted by law.“ (Signal.org, 2018-25-05, Other instances where Signal may need to share your data, signal.org, 2020-14-12, https://signal.org/legal/)
- Behandlung der Nutzerprofile (Signal.org, 2017-06-09, Encrypted profiles for Signal now in public beta, 2020-14-12, https://signal.org/blog/signal-profiles-beta/)
- Geheimdienstanfragen (Signal.org, 2016-04-10, Government Request – Grand jury subpoena for Signal user data, Eastern District of Virginia, 2020-14-12, https://signal.org/bigbrother/)
- Signal behält sich Updates der Privacy Policy vor, ohne diese aktiv jedem Nutzer bekannt zu machen.
  „Updates
  We will update this privacy policy as needed so that it is current, accurate, and as clear as possible. Your continued use of our Services confirms your acceptance of our updated Privacy Policy.“ (Signal.org, 2018-25-05, Updates, 2020-14-12, https://signal.org/legal/)

Eigenschaften

- Verschlüsselung mit Public- / Privatekey-Infrastruktur
  (Signal.org, 2018-25-05, Privacy Policy, 2020-14-12, https://signal.org/legal/)
  Auffällig hierbei ist, dass es unter der URL von Signal keine näheren Erläuterungen zum verwendeten Verschlüsselungsprotokoll gibt. Da WhatsApp angibt das gleiche Protokoll zu nutzen, können Interessierte sich die Ausführungen zu diesem Protokoll unter „WhatsApp“ ansehen. Die dazugehörige URL lautet:
  https://scontent.whatsapp.net/v/t39.8562-34/122249142_469857720642275_2152527586907531259_n.pdf/WA_Security_WhitePaper.pdf?ccb=2&_nc_sid=2fbf2a&_nc_ohc=AfJcPY3BmkMAX-Co7Ch&_nc_ht=scontent.whatsapp.net&oh=9c205cb0ec1c58c47f2eb9d0bd9a1eae&oe=5FFB6899)
- Text- und Sprachnachrichten
- Sprach- und Videoanrufe
- Gruppen und Verteilerlisten
- Desktop App
- Dateien, Medien und Standorte teilen
- ***Anmerkung***
  Am 14. Dezember 2020 um 15:02 veröffentlichte das Portal „Haaretz“ die Meldung, dass Signal von einer israelischen Sicherheitsfirma „gebrochen“ worden sei (Haaretz, 2020-14-12, Israel Spy Tech Firm Says It Can Break Into Signal App Previously Considered Safe From Hacking, 2020-15-12, https://www.haaretz.com/amp/israel-news/tech-news/.premium-israeli-spy-tech-firm-says-it-can-break-into-signal-app-previously-considered-safe-1.9368581).
  Diese Nachricht wurde jedoch von keinem der folgenden Nachrichtenseiten für IT-Sicherheit bestätigt:

- Heise Security
- Vice
- Bleeping Computer
- Netzpolitik.org – Netzpolitik stellt diese Behauptung sogar als Falschmeldung dar (Netzpolitik.org, 2020-14-12, Was sonst noch passierte, 2020-15-12, https://netzpolitik.org/2020/lockdown-s02e01/). Daher bleiben wir bei der Empfehlung von Singal.

5. Telegram

Telegram (Telegram Privacy Policy, 2020-14-12, https://telegram.org/privacy?setln=de)

(Heise Security, Telegram-Chat: der sichere Datenschutz-Albtraum - eine Analyse und ein Kommentar, 2020-14-12, https://www.heise.de/hintergrund/Telegram-Chat-der-sichere-Datenschutz-Albtraum-eine-Analyse-und-ein-Kommentar-4965774.html?seite=all)

Anonyme Nutzung: Nein

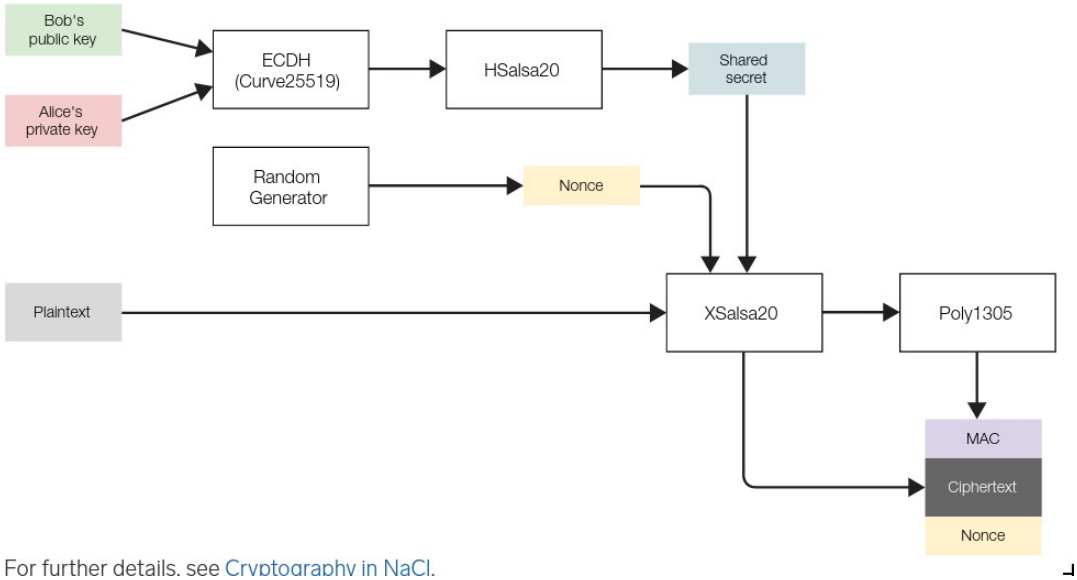
Ende-zu-Ende -Verschlüsselung:
Geheime Chats mit Ende-zu-Ende-Verschlüsselung können eingestellt und genutzt werden. Diese Chats können laut Telegram nicht mitgelesen werden und eine Speicherung dieser erfolgt ebenfalls nicht.
Medien in geheimen Chats werden mit einem separaten Schlüssel verschlüsselt, der den Servern nicht bekannt ist. Der Schlüssel und der Speicherort der Datei werden erneut verschlüsselt (mit dem Schlüssel des geheimen Chats) und an den Empfänger gesendet. Die Dateien können heruntergeladen und entschlüsselt werden.
Die Datei befindet sich auf dem Telegramserver, kann laut Telegram von niemandem, außer dem Sender und dem Empfänger gelesen werden und wird nach einiger Zeit vom Server gelöscht., um Speicherplatz zu sparen.
Dateien in öffentlichen Chats werden während des Transportes verschlüsselt, sind jedoch für alle zugänglich.
Umgang mit Metadaten:
Telegram verarbeitet personenbezogene Daten mit der Begründung, dass eine solche Verarbeitung erforderlich ist, um die Interessen Telegrams zu fördern. Diese Interessen beinhalten unter anderem: Die Bereitstellung von Telegram Diensten, Aufdeckung oder Verhinderung von Betrug und Sicherheitsproblemen.
Eine Ausnahme wäre, wenn dies mit den Interessen der Nutzer oder deren Grundrechten nicht übereinstimmt.
Genutzte Daten sind zum Beispiel die Telefonnummer, Nutzerkontodaten (Profilbild, Name, bereitgestellte Nutzerinformationen und E-Mailadresse, um ein vergessenes Passwort wiederherzustellen).
Nachrichten, Fotos und Videos werden auf Telegram Servern laut Telegram stark verschlüsselt gespeichert. Die Verschlüsselungsschlüssel werden in unterschiedlichen anderen Rechenzentren gespeichert.
Cookies werden laut Telegram zur Verbesserung der Benutzererfahrung verwendet, nicht zur Erstellung eines Nutzerprofils oder zu Werbezwecken. Werden Cookies blockiert oder deaktiviert, ist eine Anmeldung bei Telegram nicht mehr möglich.
Befindet sich der Nutzer in Großbritannien oder dem europäischen Wirtschaftsraum, werden die Daten in Rechenzentren von Drittanbietern in den Niederlanden gespeichert aber nicht an diese weitergegeben.
Die Daten werden solange gespeichert, wie zur Pflichterfüllung (Bereitstellung der Dienste) von Telegram erforderlich ist.
Metadaten, wie IP-Adresse, Geräte, Telegram-Apps und ggf. Änderung des Nutzernamens werden gespeichert und überwacht, um Missbräuche und Verstöße aufzudecken. Die Aufbewahrung erfolgt maximal 12 Monate.
Moderatoren können Nachrichten überprüfen, die von Nutzern gemeldet worden sind, um missbräuchliches Verhalten zu vermeiden.
Telegram kann automatisierte Algorithmen verwenden, um Nachrichten in Cloud Chats zu analysieren.
Geräteübergreifende Metadaten werden möglicherweise gespeichert, um Telegramfunktionen zu erstellen, die auf allen Geräten des Nutzers funktionieren.

Telegram verwendet ebenfalls Metadaten der Anwender über das Nutzungsverhalten der App. Häufig kontaktierte Personen werden analysiert, diese Funktion kann unter „Einstellungen“-„Datenschutz und Sicherheit“ – „häufige Kontakte“ deaktiviert werden.
Telegram verfügt über eine Programmierschnittstelle, mit der Drittanbieter Bots erstellen können. Diese Bots sind Apps, die wie spezielle Telegrambenutzer aussehen.
Benutzer können über die Chat-Liste mit den Bots sprechen, diese in Gruppen hinzufügen oder auf ihre Funktionen zugreifen. Wird eine dieser Aktionen durchgeführt, werden einige Daten an die jeweiligen Botentwickler gesendet.
Daten werden übertragen, wenn diese direkt an den Bot gesendet werden, wenn gemeinsam an einer Gruppe teilgenommen wird und bei Zahlungen von Dienstleistungen.
Befindet sich ein Bot in einer Gruppe, hat dieser Zugriff auf Nachrichten. Die Bots der Drittanbieter sollten den Nutzer vor dem Datenzugriff um Erlaubnis fragen.
Telegram verwaltet die Bots der Drittanbieter nicht, diese haben ihre eigenen Bots.
Der Chatverlauf in privaten Chats kann ab Version 5.5 durch einen Teilnehmer gelöscht werden. Die App wird angewiesen, alle Nachrichten des Verlaufs zu entfernen, einige werden jedoch beibehalten.
Änderungen der Datenschutzrichtlinie werden ohne vorherige Nutzerbenachrichtigung gültig.
Open Source/Closed Source:
Der Code der Telegram-Clients – nicht jedoch des Servers – ist größtenteils öffentlich verfügbar
Standort des Anbieters: Das Entwicklungsteam von Telegram hat seinen Sitz in Dubai, Die meisten Entwickler bei Telegram stammen ursprünglich aus St. Petersburg
Kosten: Telegram stellt seine Dienste kostenlos zur Verfügung.

Heise Security Bericht:
Laut des Heise Berichts aus diesem Jahr ist der Messenger Telegram nicht so sicher, wie von den Entwicklern dargestellt.
Heise hat zwei Tests durchgeführt, einmal soll ein Link zu einer Website versendet werden, der Link wird erstmal nur eingegeben aber nicht versendet. Telegram liefert alles, was eingetippt wird, ohne es versendet zu haben, bereits an den Telegam Server. Ein Test mit einer URL, die noch nirgends vorher verwendet wurde, ergab, dass lediglich beim Eintippen der URL ein Telegram Bot bereits Zugriff auf den Honey-URL-Server des Testers hatte. Die IP-Adresse des Bots kam von einem Telegram Server aus England. Das bedeutet, der Telegram Server hatte sich bereits vor dem Versenden des Links Zugang zum Nutzerserver verschafft.
Ein zweiter Test wurde gemacht, hier wurde in einem privaten Browser-Fenster die Webseite des Telegram -Chats geöffnet. Die Anmeldung dazu erfolgt über die Handynummer. Telegram versendet dann einen Login Code. Der Code wurde erhalten aber noch nicht in den Browser eingegeben. Das Handy wurde in den Flugmodus geschaltet und dennoch öffnete sich eine Webseite mit allen Chats des Nutzers.
Da sich das Handy im Flugmodus befindet, können die Chats nicht geladen werden. Da diese bei der Telegram Browser Anwendung jedoch trotzdem geladen worden sind, kommen die Chatverläufe von einem Web-Server. In diesem Test kam die IP -Adresse des Servers aus einem Rechenzentrum in Amsterdam. Der Server hat somit Zugriff auf alle Chatkopien und Nachrichten, die noch nicht versendet wurden.
Somit wird laut Heise Security alles, was die Nutzer schreiben, zentral von Telegram gespeichert und bei Bedarf ausgeliefert.
Der gleiche Test wurde mit Whatsapp gemacht, dieser hat ergeben, dass der Browser die Chatinhalte von dem Handy aus erhält, da Whatsapp Web vergeblich probiert hat, das ausgeschaltete Handy zu erreichen.

6. Threema

- Verschlüsselung mit dem NaCl (Open Source) (NaCl, 2016-15-03, NaCl: Networking and Cryptography library, NaCl: Networking and Cryptography library, 2020-14-12, http://nacl.cr.yp.to/).
  Verifikation über folgenden Link möglich (Threema, Threema Encryption Validation, 2020-14-12, https://threema.ch/validation/)
- Technische Einzelheiten der Verschlüsselung finden sich hier (Threema, Threema Cryptography Whitepaper, 2020-14-12, https://threema.ch/press-files/2_documentation/cryptography_whitepaper.pdf)
  - Asymmetrische Verschlüsselung mit Public- und Private-Key
    Private-Key wird mit Eliptic Curve (Curve25519) erstellt. Gilt als das derzeit sicherste Verschlüsselungsverfahren, abgesehen von einer vor kurzem vorgestellten Quanten sicheren Verschlüsselung, die noch nicht marktreif ist (Dezember 2020).
- „Verification Level“ von
  Rot (level 1) Der Nutzer kann sich der Identität des Absenders nicht sicher sein
  Orange (level 2) Der Threema Server hat den Absender an Hand seiner Telefonnummer oder seiner E-Mailadresse identifiziert
  Grün (level 3) Der Absender ist dem Empfänger persönlich bekannt und der Empfänger hat dies bestätigt
- Graphische Darstellung der Verschlüsselung (Threema, Threema Cryptography Whitepaper, 2020-14-12, https://threema.ch/press-files/2_documentation/cryptography_whitepaper.pdf)



Eigenschaften

- Verschlüsselung mit Public- / Private-Key Infrastruktur (Private-Key mit Eliptic Curve – Curve 25519 – das sicherste standardisierte Verschlüsselungsverfahren) (Threema, Was macht Threema sicher?, 2020-14-12, https://threema.ch/de/faq/why_secure)
- E2EE (End-to-End-Encryption – Ende-zu-Ende-Verschlüsselung)

    - gilt für die gesamte Kommunikation (Threema, Durchgängige Ende-zu-Ende-Verschlüsselung, 2020-14-12, https://threema.ch/de/security)
- Anonyme Nutzung möglich (Einziger Anbieter) (Threema, Durchgängige Ende-zu-Ende-Verschlüsselung, 2020-14-12, https://threema.ch/de/security)
- Dezentrale Architektur (Threema, Durchgängige Ende-zu-Ende-Verschlüsselung, 2020-14-12, https://threema.ch/de/security)
- Adressbuchzugriff ist optional (Threema, Durchgängige Ende-zu-Ende-Verschlüsselung, 2020-14-12, https://threema.ch/de/security)
- Verwendet „Forward Secrecy“ - bedingt, dass „zurückliegende“ Nachrichten auch nicht entschlüsselt werden können, wenn ein aktueller Schlüssel abgefangen oder gebrochen wird (Threema, Forward Secrecy, 2020-14-12, https://threema.ch/de/faq/why_secure)
- Text- und Sprachnachrichten
- Sprach- und Videoanrufe
- Gruppen- und Verteilerlisten
- Desktop App (Threema Web)
- Dateien, Medien und Standorte teilen
- Umfragefunktion
- Textformatierung möglich

7. WhatsApp

- Verschlüsselter Nachrichtenaustausch ***mit Unternehmen*** über das „Signal-Protokoll“ - Verschlüsselung von „Open Whisper Systems“ (Signal) – seit dem 01. April 2016. Bei Unternehmen kann es jedoch sein, dass die E2EE Verschlüsselung auf einem Server endet und von dort die Nachrichten „unverschlüsselt“ weitergeleitet werden. (WhatsApp, Nachrichtenaustausch mit Unternehmen, 2020-14-12, https://www.whatsapp.com/security/) „Nachrichtenaustausch mit Unternehmen“, gilt nur für die Kommunikation über die „WhatsApp Business App“.
- Zahlungen über WhatsApp ***nicht*** E2EE (WhatsApp, Zahlungen, 2020-14-12, https://www.whatsapp.com/security/).

Eigenschaften

- Verschlüsselung mit Public- / Privatekey-Infrastruktur (WhatsApp, 2020-22-10, WhatsApp Encryption Overview, whatsapp, 2020-14-12, https://scontent.whatsapp.net/v/t39.8562-34/122249142_469857720642275_2152527586907531259_n.pdf/WA_Security_WhitePaper.pdf?ccb=2&_nc_sid=2fbf2a&_nc_ohc=AfJcPY3BmkMAX-Co7Ch&_nc_ht=scontent.whatsapp.net&oh=9c205cb0ec1c58c47f2eb9d0bd9a1eae&oe=5FFB6899)
- Schlüssel bestehend aus
  - Identity Key pair aus einem Schlüsselpaar, mit Eliptic Curve Curve25519 erstellt (Wikipedia, Identity-based encryption, 2020-14-12, https://en.wikipedia.org/wiki/Identity-based_encryption)
  - Signed Pre Key – vom Identity Key signiert. Besteht aus einem Curve 25519 Key mittlerer Länge. Wird Zeit basiert gewechselt (Cryptography, 2019-24-07, Signal Protocol, how is Signed PreKey created?2020-14-12, https://crypto.stackexchange.com/questions/72148/signal-protocol-how-is-signed-prekey-created)
  - One-Time Pre Keys – eine Reihe von Curve 25519 Schlüsseln, die als „Einmal Schlüssel“ verwendet werden. (Signal, 2016-04-11, The X3DH Agreement Protocol, 2020-14-12, /signal.org/docs/specifications/x3dh/)
    Alle Schlüssel werden bei der Installation erzeugt.
  - Session Key Types
    Schlüssel für jede „Sitzung“
    Root Key (32 Byte) um *Chain Keys* zu erzeugen (PC, root key, 2020-14-12, https://www.pcmag.com/encyclopedia/term/root-key)
    Chain Key (32 Byte) wird genutzt um *Message Keys* zu erzeugen
    Message Key (80 Byte) wird genutzt um die Inhalte von Nachrichten zu verschlüsseln. Er ändert sich bei jeder Nachricht und ist *ephemeral* (Open Stack, Datenverschlüsselung, 2020-14-12, https://docs.openstack.org/de/security-guide/tenant-data/data-encryption.html) – das bedingt, dass mit einem abgefangenen Schlüssel ältere Nachrichten ***nicht*** entschlüsselt werden können. Man nennt dies auch *Perfect forward*

secracy (Wikipedia, Perfect Forward Secrecy, 2020-14-12, https://de.wikipedia.org/wiki/Perfect_Forward_Secrecy). Verbunden damit wird jeweils ein neuer *ECDH (Eliptic Curve Diffie Hellman*) Schlüssel erzeugt (Wikipedia, Eliptic-Curve Diffie-Hellman, 2020-14-12, https://en.wikipedia.org/wiki/Elliptic-curve_Diffie%E2%80%93Hellman). Die Bytes teilen sich auf in
32 Byte für einen AES256 Schlüssel – zur Verschlüsselung der Nachrichten (Wikipedia, Advanced Encryption Standard, 2020-14-12, https://de.wikipedia.org/wiki/Advanced_Encryption_Standard) im CBC Mode (Cipher Block Chaining Mode (Wikipedia, Cipher Block Chaining Mode, 2020-14-12, https://de.wikipedia.org/wiki/Cipher_Block_Chaining_Mode)
32 Byte für einen HMAC-SHA256 Schlüssel - für die Authentifikation (Wikipedia, Keyed-Hash Message Authentication Code, 2020-14-12, https://de.wikipedia.org/wiki/Keyed-Hash_Message_Authentication_Code)
16 Byte für IV (Initialisierungsvektor (Wikipedia, Initialisierungsvektor, 2020-14-12, https://de.wikipedia.org/wiki/Initialisierungsvektor)

- Text- und Sprachnachrichten
- Sprach- und Videoanrufe
- Gruppen und Verteilerlisten
- Desktop App
- Dateien, Medien und Standorte teilen
- Zahlungen über WhatsApp möglich – ***nicht*** E2EE
- Nirgends erwähnt, aber bekannt ist, dass WhatsApp die Metadaten die bei der Kommunikation anfallen kommerziell verwertet.

8. Empfehlungen

Threema	Sehr gutes Konzept, größere Reichweite, anonyme Nutzung möglich
Element	Sehr gutes Konzept, Server THL
Signal	Sehr gutes Konzept, Sitz in den USA, Beteiligung „Dritter“
WhatsApp	Nachrichten und Anrufe E2EE, aber massive kommerzielle Nutzung von Metadaten
Discord	Massive kommerzielle Verwendung sämtlicher Nutzerdaten
Messenger (Facebook)	Massive kommzerzielle Verwendung sämtlicher Nutzerdaten
Telegram	Überhaupt keine Privatsphäre, eingetippte Daten werden in Echtzeit an Telegram übertragen und dort auf unbestimmte Zeit gespeichert. https://www.heise.de/hintergrund/Telegram-Chat-der-sichere-Datenschutz-Albtraum-eine-Analyse-und-ein-Kommentar-4965774.html

9. Begründung

Vorweg eine Bemerkung zu Standorten. 2017 wurde in Amerika der ***FISA Amendments Reauthorization Act of 2017*** erlassen. In Sektion 702, § 1881a wird es amerikanischen Nachrichtendiensten erlaubt, von amerikanischen Firmen – weltweit – die Herausgabe sämtlicher Kundendaten zu verlangen, ohne dass die Kunden darüber in Kenntnis gesetzt werden dürfen. Die Kunden dürfen bis zu einem Jahr auf dieser Basis beobachtet werden (Congress.Gov, FISA Amendments Reauthorization Act of 2017, 2020-14-12, https://www.congress.gov/bill/115th-congress/senate-bill/139/text)
und (American University National Security Law Brief, 2019, Insidious Encroachment? Strengthening the "Crown Jewels": The 2018 Reauthorization of FISA Section 702, 2020-14-12, https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1108&context=nslb)
Im Zusammenhang mit dem ***Patriot Act*** (Preserving Life and Liberty, The USA Patriot Act: Preserving Life and Liberty, 2020-14-12, https://www.justice.gov/archive/ll/highlights.htm) besteht daher für „Ausländer“ in Amerika oder Kunden amerikanischer Firmen ***faktisch kein Datenschutz***.

Aus diesem Grund sind Nutzerdaten bei amerikanischen Firmen ***nie*** vor dem Zugriff durch Nachrichtendienste sicher und wir ziehen die Schweiz als Standort von Threema dem Standort USA von Signal vor.

Wir empfehlen ***Threema*** an erster Stelle, weil es eine sehr sichere Verschlüsselung anbietet. Außerdem ist es mit Threema als einzigem Anbieter möglich ***anonym*** zu kommunizieren. Das ermöglicht sonst keiner der vorgestellten Messenger. Threema arbeitet auch ***dezentral***, das macht es potentiellen Angreifern schwerer Daten zu rauben, weil sie immer nur an einen Teil herankommen. Bei Diensten, die die Daten zentral verarbeiten, reicht es aus, einen zentralen Server zu erobern. Zusätzlich hat Threema seinen Firmensitz in der Schweiz, die dafür bekannt ist, sehr gute gesetzliche Regelungen zum Datenschutz zu haben.

Element der THL ist unsere zweite Empfehlung. Es ist fast genauso gut wie Threema, bietet aber nicht die Möglichkeit anonym zu kommunizieren. Die Server der THL, damit unser IT-Support, gilt für uns als absolut vertrauenswürdig.

Signal bietet eine der sichersten Verschlüsselungen die derzeit bekannt sind an, das ***Signal Protocol*** der Firma ***Open Whisper Systems***. Es ist ein Open Source, also Quell offenes Protokoll. Das Protokoll verwendet unter anderem auch die ***Eliptic Curve Curve 25519*** – https://de.wikipedia.org/wiki/Curve25519. Eliptic Curves bieten Verschlüsselungsalgorithmen mit Nachkommazahlen, im Gegensatz zu AES oder RSA, die ganze Zahlen verwenden. Die ***Curve25519*** gilt als eine der sichersten Eliptic Curves. Sie kommt aber auch bei Threema, Element und WhatsApp zum Einsatz. Zusätzlich sind Verschlüsselungen nach AES256 und HMAC-SHA256 im Einsatz. Eine Komposition der sichersten derzeit bekannten Verschlüsselungen.

WhatsApp punktet mit der Verschlüsselung der Nachrichten mit dem ***Signal Protocol***. Was nirgends steht, aber bekannt ist, ist, dass WhatsApp die Metadaten der Nutzer kommerziell verwertet und speichert. Das sind alle Daten die neben den ***Inhaltsdaten*** anfallen. Dazu gehören der ***Standort***, wer mit wem, wann wie oft mit welchem Gerät etc., kommuniziert hat.
Der Austausch zweier E-Mails mit dem Inhalt „Das ist eine Testmail“ - Antwort: „Prima“ hat Metadaten erzeugt, die mehr als 2.000 (zweitausend) potentielle Angriffsvektoren eröffnet haben. Solcherlei Daten nutzt WhatsApp, während die vorgenannten Messenger diese sofort verwerfen.

Messenger, Discord und Telegram nutzen Daten der Nutzer in so gravierendem Umfang kommerziell und für eigene Zwecke, dass wir von deren Gebrauch abraten.

10. Quellennachweis

American University National Security Law Brief, 2019, Insidious Encroachment? Strengthening the "Crown Jewels": The 2018 Reauthorization of FISA Section 702, 2020-14-12, https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1108&context=nslb

Cryptography, 2019-24-07, Signal Protocol, how is Signed PreKey created?2020-14-12, https://crypto.stackexchange.com/questions/72148/signal-protocol-how-is-signed-prekey-created

Congress.Gov, FISA Amendments Reauthorization Act of 2017, 2020-14-12, https://www.congress.gov/bill/115th-congress/senate-bill/139/text

Discord, Datenschutzerklärung, 2020-14-12, https://discord.com/privacy

Facebook, Datenschutzerklärung, 2020-14-12, https://www.facebook.com/policy.php

Haaretz, 2020-14-12, Israel Spy Tech Firm Says It Can Break Into Signal App Previously Considered Safe From Hacking, 2020-15-12, https://www.haaretz.com/amp/israel-news/tech-news/.premium-israeli-spy-tech-firm-says-it-can-break-into-signal-app-previously-considered-safe-1.9368581

Heise Security, Telegram-Chat: der sichere Datenschutz-Albtraum - eine Analyse und ein Kommentar, 2020-14-12, https://www.heise.de/hintergrund/Telegram-Chat-der-sichere-Datenschutz-Albtraum-eine-Analyse-und-ein-Kommentar-4965774.html?seite=all

NaCl, 2016-15-03, NaCl: Networking and Cryptography library, NaCl: Networking and Cryptography library, 2020-14-12, http://nacl.cr.yp.to/

Netzpolitik.org, 2020-14-12, Was sonst noch passierte, 2020-15-12, https://netzpolitik.org/2020/lockdown-s02e01/

Open Stack, Datenverschlüsselung, 2020-14-12, https://docs.openstack.org/de/security-guide/tenant-data/data-encryption.html

PC, root key, 2020-14-12, https://www.pcmag.com/encyclopedia/term/root-key

Preserving Life and Liberty, The USA Patriot Act: Preserving Life and Liberty, 2020-14-12, https://www.justice.gov/archive/ll/highlights.htm

Signal.org, 2017-06-09, Encrypted profiles for Signal now in public beta, 2020-14-12, https://signal.org/blog/signal-profiles-beta/

Signal.org, 2016-04-10, Government Request – Grand jury subpoena for Signal user data, Eastern District of Virginia, 2020-14-12, https://signal.org/bigbrother/

Signal.org, 2018-25-05, Information you provide – Messages. signal.org, 2020-14-12, https://signal.org/legal/

Signal.org, 2018-25-05, Information you provide – Contacts, signal.org, 2020-14-12, https://signal.org/legal/

Signal.org, 2018-25-05, Signal Terms & Privacy Policy, Privacy Policy, 2020-14-12, https://signal.org/legal/#privacy-policy

Signal.org, 2018-25-05, Signal Terms & Privacy Policy, Terms of Service, 2020-14-12, https://signal.org/legal/#terms-of-service

Signal, 2016-04-11, The X3DH Agreement Protocol, 2020-14-12, /signal.org/docs/specifications/x3dh/

Telegram Privacy Policy, 2020-14-12, https://telegram.org/privacy?setln=de

The Matrix.org Foundation, An open network for secure, decentralized communication, matrix, 2020-14-12, https://matrix.org/

TH Lübeck, Datenschutzerklärung für den Chat-Dienst der Technischen Hochschule Lübeck, 2020-14-12, https://chat.stud.th-luebeck.de/daterkl.html

TH Lübeck, Nutzungsbedingungen für den Chat-Dienst Technischen Hochschule Lübeck („THL-Chat“), 2020-14-12, https://chat.stud.th-luebeck.de/nutzbed.html

Threema, Threema Cryptography Whitepaper, 2020-14-12, https://threema.ch/press-files/2_documentation/cryptography_whitepaper.pdf

Threema, Durchgängige Ende-zu-Ende-Verschlüsselung, 2020-14-12, https://threema.ch/de/security

Threema, Forward Secrecy, 2020-14-12, https://threema.ch/de/faq/why_secure

Threema, Threema Encryption Validation, 2020-14-12, https://threema.ch/validation/

Threema, Was macht Threema sicher?, 2020-14-12, https://threema.ch/de/faq/why_secure

WhatsApp, 2020-22-10, WhatsApp Encryption Overview, whatsapp, 2020-14-12, https://scontent.whatsapp.net/v/t39.8562-34/122249142_469857720642275_2152527586907531259_n.pdf/WA_Security_WhitePaper.pdf?ccb=2&_nc_sid=2fbf2a&_nc_ohc=AfJcPY3BmkMAX-Co7Ch&_nc_ht=scontent.whatsapp.net&oh=9c205cb0ec1c58c47f2eb9d0bd9a1eae&oe=5FFB6899

WhatsApp, Nachrichtenaustausch mit Unternehmen, 2020-14-12, https://www.whatsapp.com/security/

WhatsApp, Zahlungen, 2020-14-12, https://www.whatsapp.com/security/

Wikipedia, Advanced Encryption Standard, 2020-14-12, https://de.wikipedia.org/wiki/Advanced_Encryption_Standard

Wikipedia, Cipher Block Chaining Mode, 2020-14-12, https://de.wikipedia.org/wiki/Cipher_Block_Chaining_Mode

Wikipedia, Eliptic-Curve Diffie-Hellman, 2020-14-12, https://en.wikipedia.org/wiki/Elliptic-curve_Diffie%E2%80%93Hellman

Wikipedia, Identity-based encryption, 2020-14-12, https://en.wikipedia.org/wiki/Identity-based_encryption

Wikipedia, Initialisierungsvektor, 2020-14-12, https://de.wikipedia.org/wiki/Initialisierungsvektor

Wikipedia, Keyed-Hash Message Authentication Code, 2020-14-12, https://de.wikipedia.org/wiki/Keyed-Hash_Message_Authentication_Code

Wikipedia, Perfect Forward Secrecy, 2020-14-12,
https://de.wikipedia.org/wiki/Perfect_Forward_Secrecy

Zum Thema Server Encoding – Server Verschlüsselung, 2020-14-12,
https://support.discord.com/hc/en-us/community/posts/360043672952-Server-Encoding-Server-Verschl%C3%Bcsselung