TheraPsy Connect

Datenschutz White-Paper

Dieses Dokument ist ein White-Paper über den Datenschutz von der Videotelefonieplattform TheraPsy Connect. Hier fassen wir zusammen welche Schritte wir unternehmen um den Datenschutz zu gewährleisten, wie wir die Daten unserer Nutzer schützen und wie Video- und Audiodaten übertragen werden.

TheraPsy IT OG, März 2020

Kurzzusammenfassung

Der Schutz der Daten unserer Nutzer*innen und derer Klient*innen ist uns sehr wichtig. Hier ist die Kurzzusammenfassung dieses Dokuments:

- Alle Anrufe sind Ende-zu-Ende verschlüsselt. Das heißt, niemand hat Zugriff auf den Inhalt der Anrufe zwischen Therapeut*Innen und Klient*Innen.
- Wir machen und speichern keine Aufzeichnungen von Anrufen.
- Die komplette Infrastruktur von TheraPsy Connect steht im deutschsprachigen Raum. Server außerhalb dieser Region werden nicht für die Übertragung von Daten verwendet.
- TheraPsy Connect ist DSGVO konform.

Es gibt viele Anbieter für Videotelefonie und deren Produkte und Technologien ändern sich sehr schnell. Dies ist nicht als rechtliche Beratung oder als Nicht-Empfehlung zu verstehen. Wir bitten jeden sich selbst Überlegungen über diese Anbieter zu machen. Zum aktuellen Zeitpunkt stimmen folgende Informationen:

- WhatsApp: Nicht DSGVO konform [1]. Gehört zu Facebook.
- Skype: Gehört zu Microsoft.
- Zoom: Teilt Metadaten mit Facebook.

Folgende Paragraphen erarbeiten die oben zusammengefassten Informationen auf einer tiefergehenden technischen Stufe und geben mehr Details bekannt.

1. Einleitung

TheraPsy Connect ist eine Videotelefonieplattform der TheraPsy IT OG, welche es Nutzer*innen erlaubt psychotherapeutische Arbeit mittels Online-Videotelefonie durchzuführen [2]. Uns ist natürlich bewusst, dass vor allem im Gesundheitsbereich der Datenschutz absolut essentiell und nicht wegzudenken ist. Dieses Dokument beschreibt die Architektur des Systems und beleuchtet die Maßnahmen, welche wir unternehmen, um diesen zu Recht hohen Anforderungen des Datenschutzes gerecht zu werden.

2. Funktionsweise

TheraPsy Connect verwendet im Hintergrund die Vonage Video API [3]. Vonage ist ein etabliertes Unternehmen, welches verschiedene Technologien zur Onlinekommunikation zur Verfügung stellt. Die unterliegende Technologie dahinter ist WebRTC, welche ein anerkannter offener Standard von W3C ist. Die Videotelefonie findet, wenn möglich, mittels Direktverbindungen („Peer to Peer“) statt. Es gibt Situationen, welche dies aufgrund von Firewall-Einstellungen nicht möglich machen. In diesen Fällen wird ein Zwischenserver verwendet, der die Kommunikation zwischen den beiden Geräten der Endnutzer ermöglicht. In allen Fällen sind die Video- und Audiodaten immer Ende-zu-Ende verschlüsselt.

3. Datenschutzmaßnahmen von TheraPsy Connect

Wie bereits erwähnt werden alle Anrufe immer Ende-zu-Ende verschlüsselt. Dafür wird aktuell der AES Algorithmus (128 bit Variante) verwendet. Um die Anrufe aufzusetzen wird ein Server als initialer Kontaktpunkt („Signaling Server") benötigt, damit die jeweiligen Geräte wissen mit wem sie kommunizieren müssen. Dieser Server wird im Laufe des Gesprächs für Folgendes verwendet:

1. In regelmäßigen Abständen (ca. 10 Minuten) wird die Verschlüsselung erneuert.
2. Qualitätsmanagement: TheraPsy Connect kommuniziert mit dem Gegenüber und verständigt sich in welcher Qualität die Video- und Audiodaten gesendet werden können um ein flüssiges Gespräch aufrechtzuerhalten.

Die Anrufe geschehen in einer von zwei Arten:

1. „Peer to Peer": Wenn möglich werden die Daten direkt zwischen den Teilnehmern versendet. Dies ist immer dann möglich, wenn beide Endgeräte die eigene öffentliche IP Adresse kennen, was in rund 70% der Fall ist. (Quote hängt stark vom Umfeld ab). Bei Privatpersonen ist dies meist der Fall. Sollten Firewall Einstellungen dies nicht erlauben, wird der zweite Modus verwendet.
2. TURN-Modus: Wenn mindestens eines der Endgeräte die öffentliche IP Adresse nicht kennt, wird ein TURN Server von Vonage verwendet, welcher keinen Zugriff auf die eigentlichen Video- und Audiodaten hat, sondern lediglich die Daten an die andere Partei weiterleitet. Dies ist mittels mehrschichtigen Verschlüsselungsprotokollen sichergestellt. Der Turn Server liest/verwendet nur die UDP Schicht, hat aber keinen Zugriff auf die DTLS Verschlüsselung [4].

Sämtliche Server in dieser Kommunikationskette (TURN und Signaling Server) befinden sich in Deutschland (Frankfurt). Alle Server, welche in Deutschland von Vonage verwendet werden sind ISO 27001 zertifiziert [5,6]. Sämtliche Dienste von Vonage sind DSGVO konform. Sollten verwendete Server nicht zur Verfügung stehen, werden andere Server in Deutschland zum Ausweichen verwendet. Wenn innerhalb von Deutschland keine Server zur Verfügung stehen, werden keine Server im Ausland verwendet.

Während Anrufen werden Metainformationen (Bitraten, Fehler in den Verbindungen, ...) gespeichert, welche keinen Rückschluss auf die teilnehmenden Personen erlauben. Dies erlaubt es uns die Qualität sicherzustellen und Serverauslastungen zu kontrollieren.

Von sämtlichen Anrufen werden von den Inhalten des Gesprächs keine Aufzeichnungen gemacht (weder Video, noch Audio). Dies wäre bei einer Ende-zu-Ende Verschlüsselung ohnehin nicht möglich.

Anwenderdaten:

Um die Dienstleistungen von TheraPsy Connect sicherzustellen, müssen gewisse Daten gespeichert werden. Aktuell befinden sich die entsprechenden Server in Frankfurt.

Im Zuge eines TheraPsy Connect Anrufs werden folgende Daten in SQL Datenbanken gespeichert:

- Authentifizierungstokens
- Klient*innen ID (vom Nutzer eingegeben)
- TherapeutInnen Code (meist Nutzername des TheraPsy Nutzers / der TheraPsy Nutzerin)
- Erstellzeitpunkt der Session

Sofern die von dem/der Therapeut*in eingegebene Klienten ID keinen Rückschluss auf die Klient*in erlaubt, lassen sämtliche gespeicherte Daten keinen Rückschluss auf die Klient*in zu.

Während des Anrufs werden in derselben Datenbank Ereignisse wie Verbindungsherstellungen und Abbrüche gespeichert, da die für eine spätere Verrechnung notwendig sind.
Diese Daten werden in keiner Weise mit Drittpersonen geteilt und von uns ausschließlich für funktionale Zwecke von TheraPsy Connect verwendet.

4. Vergleich

Der Online-Videotelefoniemarkt ist stark umkämpft. Nicht alle Anbieter nehmen den Datenschutz dabei so ernst wie wir dies tun.

1. WhatsApp Videotelefonie: WhatsApp ist nicht DSGVO konform [1]. Als Tochterunternehmen von Facebook können Daten zwischen der Mutter und Tochtergesellschaft jederzeit übertragen werden. WhatsApp lädt Daten von Drittpersonen ohne deren Einverständnis hoch.
2. Zoom: Zoom geriet in Kritik für die Art und Weise wie Daten mit Facebook geteilt werden. Die iOS Zoom App teilt Facebook mit, wann die App geöffnet wurde, Netzwerkanbieter, Zeitzone des Orts, etc. [7]. Dies passiert unabhängig davon, ob man einen Facebook Account hat oder nicht. Diese Daten sind sehr wahrscheinlich nicht sehr sensitiv, dennoch wurde die Dienstleistung von mehreren Regierungen für interne Zwecke pausiert [8].
3. Skype: Gehört zu Microsoft und wurde in Vergangenheit bereits datenschutztechnisch kritisiert [9].

5. Abschluss

In diesem Dokument haben wir Systemarchitekturen und Datenschutzmaßnahmen transparent gemacht. Falls konkretere Informationen gewünscht sind, kann mit uns Kontakt aufgenommen werden. Wir hoffen, dass dieses White-Paper die Datenschutzmaßnahmen klarstellt und deutlich macht, dass wir uns aktiv um dieses Thema kümmern.

TheraPsy Connect befindet sich nie im Stillstand, da wir konstant an allen Ecken und Enden weiterarbeiten. In der Entwicklung wird die Sicherheit der Daten von Beginn an als oberste Priorität berücksichtigt.

Quellen:

[1] https://easygdpr.eu/de/gdprfaq/ist-whatsapp-dsgvo-konform/

[2] www.therapsy.at

[3] https://www.vonage.com/communications-apis/video

[4] https://webrtc-security.github.io/

[5] https://www.vonage.com/communications-apis/platform/gdpr/sub-processors/

[6] https://d1.awsstatic.com/certifications/iso_27001_global_certification.pdf

[7] https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account

[8] https://metro.co.uk/2020/03/25/concern-zoom-video-conferencing-mod-bans-security-fears-12455327/

[9] https://www.ht4u.net/news/31792_fraunhofer_institut_aeussert_klare_sicherheitsbedenken_gegenueber_skype/

Datenschutzerklärung Vonage Inc.:
https://www.vonage.com/privacy-policy
https://tokbox.com/developer/guides/security/

Datenschutzerklärung TheraPsy:
https://www.therapsy.at/dataPolicy.php