Instahelp setzt auf modernste Datenschutzstandards

Mit Instahelp, der Plattform für psychologische Online-Beratung, bieten wir eine anonyme Möglichkeit für Personen, sich mit privaten und beruflichen Anliegen und Problemen an erfahrene Psycholog:innen zu wenden. Unsere Psycholog:innen helfen Kund:innen via Text-Chat, Audio oder Video, durch Selbsthilfe zu Lösungen zu finden und die eigene Persönlichkeit weiterzuentwickeln. Diese Kommunikation baut auf einem enormen Vertrauensverhältnis auf, das mit allen Möglichkeiten geschützt werden muss. Aus diesem Grund wurden für Instahelp drei unterschiedliche Sicherheitsmechanismen umgesetzt, welche die sensiblen Nachrichten vor Zugriff von außen schützen.

3-fache Sicherheit für Instahelp Nachrichten:

1. Verschlüsselung der Daten vor dem Versand (Ende-zu-Ende-Verschlüsselung)
2. Abgesicherte Datenübertragung (TLS)
3. Zwei-Faktor-Authentifizierung (2FA)

1. Verschlüsselung der Daten vor dem Versand

Bei Instahelp werden alle Nachrichten zwischen Kund:innen und Psycholog:innen mit einem geheimen Raum-Schlüssel verschlüsselt. Dieser geheime Raum-Schlüssel wird von Instahelp automatisch für jeden privaten Beratungsraum einmalig auf dem Gerät des:r Kund:in generiert. Damit der:die Kund:in sich den geheimen Raum-Schlüssel nicht merken muss, wird dieser wiederum verschlüsselt auf dem Instahelp Server gespeichert. Zur Verschlüsselung des geheimen Raum-Schlüssels wird das persönliche kryptografische Schlüsselpaar (privater und öffentlicher Schlüssel) des Nutzers oder der Benutzerin verwendet. Dieses Schlüsselpaar wird auf Basis des Nutzer:in-Passworts generiert und ist somit - aus technischer Sicht - nur dem:der Nutzer:in „bekannt".

Wird dem:der Kund:in ein:e Instahelp Psycholog:in in seinem privaten Beratungsraum zugewiesen, benötigt diese:r den geheimen Raum-Schlüssel, um die Nachrichten entschlüsseln zu können. Hierfür wird der persönliche öffentliche Schlüssel des:der Psycholog:in gemeinsam mit der Anfrage um Freigabe des geheimen Raum-Schlüssels an den:die Kund:in übermittelt. Sofern der:die Kund:in online ist, verschlüsselt Instahelp nun den geheimen Raum-Schlüssel mit dem öffentlichen Schlüssel des:der Psycholog:in und sendet diesen über die gesicherte Verbindung zurück. Nun wird der geheime Raum-Schlüssel mit dem privaten Schlüssel des:der Psychologin (den nur er:sie „kennt") entschlüsselt, mit welchem wiederum die Nachrichten entschlüsselt und angezeigt werden können.

Zur besseren Verständlichkeit gibt es hier ein einfaches Beispiel:

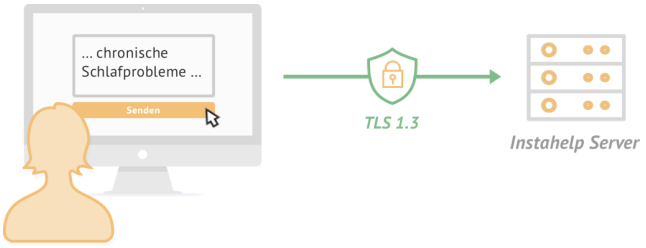
Der:Die Kundin schreibt eine Chat-Nachricht: „... chronische Schlafprobleme ..." Zum Absenden der Nachricht klickt er auf den Button „Senden". Bevor die Nachricht verschickt wird, verschlüsselt die Instahelp App die Nachricht mit dem geheimen Raum-Schlüssel.

1. Die verschlüsselte Nachricht wird nun an den Instahelp Server übertragen und in der Datenbank verschlüsselt gespeichert "%&A(!)A019!1#2%". Die ausfallsicheren Instahelp Server befinden sich im Datencenter eines europäischen Cloud-Anbieters in Deutschland (Frankfurt) und unterliegen dem deutschen Datenschutz.
2. Der:Die zugewiesene Instahelp Psycholog:in fordert nun die neue Nachricht beim Instahelp Server an und bekommt die verschlüsselte Nachricht an seinen:ihren Computer geschickt. Da der:die Psycholog:in im Besitz des gemeinsamen geheimen Raum-Schlüssels ist, kann er:sie die Nachricht entschlüsseln und lesen.

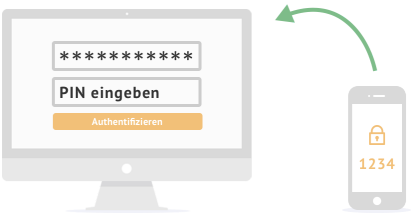
2. Gesicherte Datenübertragung

Obwohl die Nachrichten bereits verschlüsselt sind, werden sie zusätzlich über eine gesicherte Datenverbindung zum Instahelp Server übertragen. Hierfür wird der Industrie Standard TLS 1.3 (Transport Layer Security) verwendet, um die folgenden Sicherheiten zu gewährleisten:

- Für die Verbindung zum Instahelp Server wird ein Einmal-Schlüssel (256 Bit) erzeugt, der zwischen dem:der Kund:in und dem Instahelp Server automatisch digital ausgetauscht wird. Die zu sendenden Daten werden vor dem Versand mit diesem Einmal-Schlüssel verschlüsselt und an den Instahelp Server geschickt.
- Für jede gesendete Nachricht wird zusätzlich ein einmaliger Nachrichten Authentitäts-Code (=Sequenz) generiert und nach erfolgreicher Übertragung deaktiviert.



3. Zwei-Faktor-Authentifizierung (2FA)



Mit der dritten Sicherheitsmaßnahme stellen wir sicher, dass die in die Kommunikation involvierten Gesprächspartner:innen tatsächlich die Kontoinhaber:innen repräsentieren. Für diesen Zweck wurde eine Zwei-Faktor-Authentifizierung implementiert. Diese zwei Faktoren sind stellvertretend für zwei Eigenschaften, welche die Person wissen und besitzen muss. Das Wissen bezieht sich auf die Eingabe des selbst festgelegten Passworts. Der Besitz erfordert ein Smartphone mit Authentifizierungsapp oder ein Gerät mit biometrischer Erkennung mittels Passkey-Technologie. Somit muss der:die Instahelp Psycholog:in das Passwort wissen und sich über seine biometrischen Daten (oder den Code einer Authentifizierungsapp) identifizieren, um sich erfolgreich einzuloggen.

Häufige Fragen

Warum werden die Nachrichten am Instahelp Server gespeichert?
Mit Instahelp verfolgen wir das Ziel, psychologische Beratung in den Alltag zu integrieren. Der:Die Psycholog:in soll jederzeit und von überall aus erreichbar sein. Kund:innen können sich jederzeit auf dem Smartphone, Tablet oder auch am Computer bei Instahelp einloggen, um den Chat-Verlauf sowie auch neue Antworten des:der Psycholog:in einzusehen und auch sofort darauf zu antworten. Hierfür werden die Chat-Nachrichten am Instahelp Server verschlüsselt gespeichert, um jederzeit abrufbar zu sein.

Wie werden die Nachrichten verschlüsselt?
Zur Verschlüsselung der Daten wird die weit verbreitete und anerkannte LibSodium Kryptographie-Bibliothek verwendet. Jede einzelne Chat-Nachricht wird mit einem symmetrischen Raum-Schlüssel auf Basis des Verfahrens XSalsa 20 verschlüsselt. Zusätzlich wird jede Nachricht nach der Übertragung auf Manipulationen überprüft, mittels Authentifizierung der Nachricht über Poly 1305 MAC.

Was passiert, wenn ein:e Hacker:in alle Daten vom Instahelp Server stiehlt?
Falls ein:e Hacker:in alle Sicherheitsmechanismen unseres Datencenters durchbricht, findet er:sie nur unlesbare verschlüsselte Nachrichten vor. Da jede:r Kund:in bei Instahelp seinen eigenen geheimen Raum-Schlüssel verwendet, müsste der:die Hacker:in pro Kund:in versuchen, den Schlüssel zu knacken.

Wie gelange ich zu einem geheimen Raum-Schlüssel mit dem:der Psycholog:in? Muss man sich diese merken?
Nein, Instahelp verwendet ein ausgeklügeltes System, um den einmalig generierten geheimen Raum-Schlüssel wiederherzustellen. Zunächst wird das beim Login eingegebene Passwort in Kombination mit einem Zeichenzusatz vom Server (SALT) mit einer Hash-Funktion (Salsa 20/8 + SHA-256) zu einer langen Zeichenfolge (=Digest) konvertiert. Der SALT wird verwendet, um ein einfaches Passwort durch Hinzufügen einer langen zufälligen Zeichenfolge komplexer zu machen. Der Vorteil der Hash-Methode ist, dass der generierte Digest (=Zeichenfolge) nicht mehr auf die ursprünglichen Zeichen zurückgeführt werden kann und somit das Passwort des:der Nutzer:in nicht am Instahelp Server gespeichert werden muss. Mit diesem Digest wird nun der private und öffentliche Schlüssel (Curve25519 (Key exchange) + XSalsa 20 (Encryption) + Poly 1305 MAC (Authentication)) des Nutzers bzw. der Nutzerin generiert. Dieses Schlüsselpaar kann nun den vom Instahelp Server angeforderten verschlüsselten Raum-Schlüssel entschlüsseln.

Gibt es auch Inhalte, die nicht Ende-zu-Ende verschlüsselt werden?
Ja, es gibt auch Inhalte, die nicht Ende-zu-Ende verschlüsselt werden. Als Begleitung und Ergänzung zur Beratung steht registrierten Kund:innen das Mental Health Gym zur Verfügung, in dem mehrere Funktionen (z.B. Übungen, Videos oder Audio-Dateien) zur Stärkung der mentalen Gesundheit genutzt werden können. Die Daten werden nicht an Dritte weitergegeben und verschlüsselt auf unserem Server abgelegt. Anders als bei Nutzung unseres Text-Chats besteht jedoch keine Ende-zu-Ende-Verschlüsselung. Dadurch können wir auch außerhalb eines Beratungsraums die Durchführung von diversen Übungen ermöglichen. Diese Daten können somit von auch auf einem anderen Endgerät abgerufen werden und sind damit auch verfügbar, sollte das Passwort zurückgesetzt werden.