HOCCER

ende

- FAQ

Datenschutz- und Sicherheitserklärung

Hoccer ist ein Kommunikationsservice, der größten Wert auf den Schutz deiner Privatsphäre legt und Nachrichten aller Art mit einem größtmöglichen Maß an Sicherheit übermittelt (Ende-zu-Ende Verschlüsselung). Dazu benötigt Hoccer keinerlei sensible oder private Daten wie Telefonnummer oder E-Mail-Adresse. Deine Identität ist für uns nur eine zufallsgenerierte Zahl.

Das deutsche Datenschutzrecht verlangt, dass ein Service anonym oder unter einem Pseudonym genutzt werden kann. Mit dieser Regelung sind wir zu 100% konform. Um deine Nachrichten verschlüsselt zu

verschicken, bekommt jeder User eine zufallsgenerierte Nummer als Pseudonym zugewiesen, eine sogenannte „Client ID“. Diese dient zur reinen technischen Abwicklung unseres Services.

Umgang mit Userdaten

Wenn du Hoccer nutzt, werden verschiedene Daten übermittelt. Alle Daten, die wir dabei einsehen können, haben wir hier aufgelistet:

- die IP-Adresse des mit Hoccer verbundenen Gerätes (ausschließlich bei Nutzung des Services) oder die IP-Adresse des Routers, im Falle der Nutzung eines NAT Netzwerks. Dies ist in der Regel der Fall, wenn das Endgerät mit einem WLAN Netz verbunden ist
- die IP-Adresse deines Kommunikationspartners, wenn dieser online ist
- Die Menge an Daten, die übermittelt wird
- Die Uhrzeit, zu der eine Nachricht versendet und empfangen wird
- Die Uhrzeit, zu der du dich einloggst und ausloggst
- Der verwendete öffentliche Schlüssel (es gibt noch einen weiteren privaten)
- Das verwendete Betriebssystem und die verwendete Version deines Endgeräts
- Eine zufallsgenerierte Nummer, die deine Client-ID darstellt
- Der gewählte Benutzername
- Das von dir bestimmte Profilfoto

Auf Dauer wird lediglich deine Client-ID gespeichert. Dies ist notwendig, um deine Beziehung zu anderen Client-IDs korrekt wiederzugeben, wie z.B.:

- Freundschaften (verbunden mit / blockiert mit)
- Gruppenmitgliedschaften
- Profiländerungen von Freunden- oder Gruppenbildern

Profilfoto, Benutzername und der öffentliche Schlüssel können von dir jederzeit geändert und aktualisiert werden.

Diese Daten werden ausschließlich genutzt und abgefragt, um die Betriebsfähigkeit unseres Services zu garantieren. Alle anderen Daten werden für den maximal kürzesten Zeitraum gespeichert, um Nachrichten zu übermitteln. Nach abgeschlossener Übermittlung werden diese umgehend vom Server gelöscht. Wir speichern so wenige Daten wie möglich. Dies dient zum einem dem Schutz deiner Privatsphäre, zum anderen zur Kosten- und Leistungsoptimierung. Im Normalfall werden keine Log-Daten gespeichert. Dies geschieht, wenn überhaupt, nur kurzzeitig, falls Fehler im System auftreten sollten oder um die Leistung unseres Services zu optimieren.

Wir wissen nichts über den Inhalt deiner Nachrichten, ausschließlich deren Größe ist uns bekannt. Wir kennen weder den Datentypen, noch den Namen des Anhanges, den du verschickst. Alle Daten verlassen dein Telefon mit einem verschlüsselten, zufällig erstellten 256 AES Schlüssel, der dem Empfänger ebenfalls verschlüsselt (mit einem Öffentlichen RSA Schlüssel) zur Entschlüsselung deiner Nachricht übermittelt wird.

Wir kennen keinerlei Telefonnummern von dir oder deinen Freunden und haben auch keinen Zugriff auf deine E-Mail-Adressen. Wenn du eine Einladung per SMS oder E-Mail verschickst, geschieht dies außerhalb von Hoccer. Somit wissen, übermitteln oder speichern wir diese sensiblen Daten zu keiner Zeit, da wir nicht mit Ihnen in Berührung kommen und dies auch nicht wollen.

Du kannst Hoccer z.B. Zugriff auf dein Adressbuch und deinen Standort erlauben, um diese als Anhang zu verschicken. Diese werden dann sofort verschlüsselt und keinerlei Informationen werden an uns

übermittelt.

Genutzte Verschlüsselungen für Hoccer

Zunächst verwenden wir SSL/TLS Verschlüsselung für alle Verbindungen vom User zum Server sowie zwischen unseren Servern. Wir nutzen sogenannte „Pinned Certificates“, um nicht auf die herkömmliche Kette von Webbrowsern vertrauen zu müssen, weil wir diese als lückenhaft einschätzen. Es gibt zu viele Behörden, die Zertifikate ausstellen. Viele dieser Behörden sind korrupt, können überlistet werden oder geben freiwillig Zertifikate an Länder mit niedrigeren Datenschutzbestimmungen heraus.

Um „Man in the Middle – Attacken“ zu verhindern, umgehen wir diese Zertifikate. Somit sind sogar unsere Metadaten, die wir oben aufgelistet haben, äußerst sicher vor unerwünschten Zugriffen durch Dritte.

Ende-zu-Ende Verschlüsselung der Hoccer Nachrichten

Wir nutzen Ende-zu-Ende Verschlüsselung, um deine Inhalte sicher zu übermitteln: Wir nutzen RSA2048 BIT (optional bis zu 4096 BIT) als öffentliche Schlüssel in Kombination mit AES256, um deine Daten so zu verschlüsseln, dass wirklich nur der gewünschte Empfänger diese lesen kann. Nachrichten (Nutzer zu Nutzer) werden mit einem einzigartigen 256 BIT AES Schlüssel versehen. Für jede einzelne Nachricht wird hierbei ein neuer Schlüssel vergeben. Dieser Schlüssel wird mit der verschlüsselten Nachricht nochmals verschlüsselt (mit den 2048-4096 BIT RSA öffentlichen Schlüsseln des Empfängers). Der private Schlüssel (um das Gegenstück zu entschlüsseln) bleibt immer auf dem Gerät und verlässt dieses niemals.

Gruppenchats werden ähnlich verschlüsselt, nur der AES Schlüssel wird in diesem Fall mit allen Gruppenmitgliedern geteilt. Dieser Schlüssel wird mit Erstellung der Gruppe vom Admin generiert und an alle Mitglieder verschlüsselt (mit deren öffentlichem RSA Schlüssel) weitergegeben.

Die RSA Schlüssel können jederzeit manuell erneuert werden. Das System überwacht und steuert automatisch die Verteilung dieser neu angelegten Schlüssel. Ein Nummernzeichen des öffentlichen Schlüssels (Schlüssel ID) wird in jedem Kontakt im Kontaktprofil angezeigt. Für ein Extra an Sicherheit kannst du dein Nummernzeichen mit deinem Chatpartner vergleichen.

Wir geben unser Bestes, um sicherzustellen, dass die Inhalte deiner Nachrichten sicher vor unerwünschten Lesern sind und dass ausschließlich der angegebene Empfänger diese lesen kann. Uns sind keinerlei Methoden bekannt, die Lauschangriffe über deine Internetverbindung zulassen könnten und es möglich machen, Zugriff zu den Inhalten deiner Hoccer Nachrichten zu erlangen. Auch wenn neueste Erkenntnisse zeigen, dass es einige wenige Schwachstellen in der RSA und AES Verschlüsselung gibt, ist eine erfolgreiche Attacke auf Hoccer und dessen Inhalte sehr unwahrscheinlich und extrem aufwändig.

Selbst mächtige Autoritäten, wie z.B. Vollzugsbehörden, Militär oder andere autorisierte Behörden, mit der Fähigkeit den Internetverkehr zu manipulieren, können höchstwahrscheinlich keinen Zugriff auf deine Nachrichten erhalten. Eventuell können sie durch Verkehrsanalysen und Überwachung der Zeit und der Größe der Daten, die du mit deinem Chatpartner über Hoccer Server austauschst, herausfinden, mit wem du kommunizierst. Selbst dies wird nahezu unmöglich, wenn du nur Textnachrichten austauschst und du und dein Chatpartner, niemals zur gleichen Zeit online seid.

Bitte beachte jedoch, dass Hoccer nur so sicher sein kann, wie es dein Endgerät und das deines Chatpartners zulassen – inklusive aller Sicherheitsbackups, die du erstellst. Falls die Integrität eines Gerätes durch Schadensprogramme aufgehoben ist, vom Hersteller Hintertürchen eingebaut wurden oder

dein Gerät verloren geht, können auch Hoccer Inhalte gefährdet sein.

Der „in der Nähe“ Modus

Während du den Hoccer “in der Nähe” Modus verwendest, schickt dein Client deine Standortdaten an einen Hoccer Server. Diese sind auf dem Transportweg verschlüsselt, werden aber auf dem Server entschlüsselt und verarbeitet. Sie werden ausschließlich übertragen, damit du Leute in deiner Nähe sehen kannst, die ebenfalls den „in der Nähe“ Modus aktiviert haben. So kannst du dich an Gesprächen beteiligen, ohne mit den Kontakten in der Nähe befreundet zu sein. Sobald du diesen Modus verlässt, werden deine Standortdaten umgehend von den Hoccer Servern entfernt. Alle Nachrichten und Anhänge werden auch im “in der Nähe” Modus zusätzlich mit Hoccers allgemeinen Ende-zu-Ende Sicherheitsvorkehrungen geschützt. Bitte beachte aber, dass bei der Kommunikation über die „in der Nähe“-Gruppe jederzeit neue MItglieder in der Gruppe erscheinen und Nachrichten mitempfangen können. Zur Übertragung vertaulicher Daten über die „in der Nähe“-Funktion solltest du direkt in einen Chat mit dem gewünschten Kontakt eintreten, der unterhalb der „nearby“-Gruppe gelistet ist.

Server-Sicherheit

Zunächst sammeln und speichern wir so wenige Daten wie möglich. Einfach gesagt: Auf unseren Servern ist nicht viel zu holen, da keine relevanten Daten gespeichert werden, die für Angreifer von Interesse sein könnten. Die einzigen Nachrichtendaten, die auf den Servern abgelegt werden, sind die, deren Übermittlung noch nicht abgeschlossen ist. Diese vorgehaltenen Nachrichten sind selbstverständlich verschlüsselt.
Die Daten, die den höchsten Wert haben, sind die User Account-Daten. Da aber alle Passwörter automatisch generiert wurden und eine zufällige Zahlenfolge aufweisen, stellt dies selbst bei Verlust kein großes Risiko für den Account-Inhaber dar. Dies ist nur ein Problem, wenn (wie man es von anderen Serviceanbietern kennt) Passwörter geklaut werden, die vom User selbst generiert wurden und der User öfters ein und dasselbe Passwort im Netz benutzt.

Dennoch wollen wir nicht, dass jemand mit unseren Servern Schindluder betreibt. Darum treffen wir angemessene Sicherheitsvorkehrungen, um unsere Server zu schützen. Hier sind einige Sicherheitsmaßnahmen, die wir getroffen haben:

- Die Systemsoftware halten wir immer auf dem neuesten Stand
- Es werden keine unnötigen Operationen auf unseren Servern ausgeführt
- Wir überwachen mit Hilfe von automatisierten Werkzeugen Veränderungen der Software und der Konfiguration
- Wir erstellen weder System logs noch legen wir diese auf unseren Servern ab
- Wir schalten uns nicht als Superuser ein
- Nur personalisierte Zugänge für client certificates
- Wir überwachen jegliche Aktivität auf unseren Servern
- und mehr

Die einzig erfolgreiche Methode um unser System zu infiltrieren, wäre es unseren Client Code zu sabotieren. Dies würde jedoch sehr schnell auffallen und ist für den Angreifer nur mit sehr hohem Kostenaufwand durchführbar.

Ein durchaus mögliches Szenario wäre eine Attacke auf dein Endgerät. Bösartige Software könnte Screenshots von deinen Nachrichten machen und diese an den Angreifer weiterleiten. Dann kann der Angreifer auch mithören, was du zum Beispiel in Gegenwart deines Telefons sagst. In diesem Fall ist die ganze Infrastruktur deines Endgerätes gefährdet und somit auch Hoccer.

Kannst du uns vertrauen?

Wir nutzen ein eigenentwickeltes Kommunikationsprotokoll, dessen Source Code nicht öffentlich ist; alle Nachrichten laufen über unsere Server – also warum solltest du uns vertrauen? Wie kannst du dir sicher sein, dass es keine Hintertüren in unserem System gibt und wir deine Nachrichten nicht direkt in eine staatliche Datenbank weiterleiten? Ehrlich gesagt kannst du dir da nie sicher sein. Bis zu einem gewissen Punkt, musst du uns einfach vertrauen und wir hoffen, dass du dies auch tun wirst! Eines unserer Beweggründe Hoccer zu entwickeln war nämlich genau dieses fehlende Vertrauen in bestehende Messaging Services, die eine ordentliche Vielfalt an Funktionen bieten, sichere Datenübertragung versprechen und die dennoch einfach zu nutzen sind. Hoccer hätte keinen berechtigten Daseinsgrund, wenn wir die Sicherheit und Privatsphäre unserer User in irgendeiner Weise in Gefahr bringen würden. Denn dies macht uns einzigartig.

Hier eine Liste von Gründen, die dich überzeugen sollen, warum du Hoccer vertrauen kannst:

1. Du musst zu keiner Zeit Angaben zu deiner Person machen oder etwas über deine Identität aussagen
2. Wir als Entwickler sind sehr stolz darauf, eine sichere Umgebung geschaffen zu haben. Es widerstrebt uns zutiefst viel Zeit und Herzblut in Hoccer gesteckt zu haben und dann alles zunichte zu machen, indem wir Hintertürchen einbauen.
3. Die Zukunft unseres Unternehmens hängt von der Vertrauenswürdigkeit von Hoccer ab. Somit machen wir alles, um uns dieses Vertrauen ehrlich zu verdienen.
4. Das deutsche Datenschutz- und Wettbewerbsrecht ist sehr strikt und gemäß diesen Gesetzen steht auf Verstöße nach dem Bußgeldkatalog §202a sogar eine Gefängnisstrafe, wenn wir uns unautorisierten Zugang zu deinen Daten verschaffen würden.
5. Das System so sicher und Privatsphäre-schützend wie möglich zu halten, reduziert auch unseren Verantwortungsdruck bzw. unsere Risiken. Wenn wir Zugang zu deinen Nachrichteninhalten hätten, wären wir einem höheren Risiko von Attacken ausgesetzt, die sich dann Zugriff zu deinen Daten verschaffen könnten. Man kann nichts verlieren, was man nicht besitzt. Ein weiterer Pluspunkt unserer Ende-zu-Ende Verschlüsselung ist, dass wir uns nicht sorgen müssen, was über unsere Server läuft – denn wir können es einfach nicht nachvollziehen. Alles was dein Handy verlässt und auf unserem Server ankommt, ist ein nicht lesbares Bündel von Daten und Zeichen, das erst und ausschließlich auf dem Gerät des Empfängers leserlich wird.

Warum brauche ich den Schutz durch eine Ende-zu-Ende Verschlüsselung?

Viele Nutzer wollen keinen extra Aufwand in Kauf nehmen für mehr Sicherheit, da wir die meiste Zeit davon ausgehen, dass unsere alltäglichen Gespräche nicht von großem Interesse für andere sind. Wir nehmen es als gegeben hin, dass die Sicherheit des Systems, das wir nutzen, für unsere Zwecke gut genug ist …

Das mag manchmal zustimmen und manchmal … auch nicht. Bei vielen anderen Chatanbietern können Nachrichten und Anhänge nicht nur vom Serviceprovider gelesen und gespeichert werden, in manchen Fällen sogar auch von diversen Geräten, die als Knotenpunkt dienen, um die Nachricht zum Empfänger weiterzuleiten. Speicherkapazitäten im Internet sind günstig und so ist es gut möglich, dass eine Nachricht, die du heute schreibst, in 20 Jahren irgendwo auftaucht.

In unseren Augen solltest du dir keine Sorgen machen müssen, ob dein Liebesbrief, deine Ängste, deine Sorgen, deine Wut, deine Termine, deine finanziellen Überlegungen, deine Bilder, deine eigenen Videos, deine politische oder religiöse Ausrichtung, oder was auch immer du mit deinen Freunden und deiner Familie vielleicht teilen möchtest, auf Datenbanken von Leuten langfristig gespeichert wird, die du noch

nie zuvor in deinem Leben gesehen hast.

Wir können nicht garantieren, dass Hoccer absolut sicher ist. Jeder, der so etwas über sein System sagt, lügt. Was wir dir aber guten Gewissens versprechen können ist:

Bei der Nutzung von Hoccer kann nur der ausgewählte Empfänger deine Nachricht lesen und weder wir, noch irgendein Lauscher im Internet, kann Zugang zu deinen Nachrichten bekommen.

Welchen Preis zahle ich für das Extra an Sicherheit?

Sicherheit und Privatsphäre sind wesentliche Bestandteile unserer Produkte und dies wird so bleiben – kostenfrei. Auch wenn wir in Zukunft kostenpflichtige Zusatzdienste anbieten werden, wird es immer eine kostenlose Version von Hoccer geben.

Der Preis, der für das „Mehr“ an Sicherheit bei Hoccer bezahlt wird, ist eine etwas länger dauernde Verbindung zum Server (Anmeldung) als bei weniger sicheren Messengers. Die Schlüsselverteilung für den Nachrichtentransport, sowie der sichere Login können etwas Zeit in Anspruch nehmen, aber bei einer guten Internetverbindung wirst du davon so gut wie nichts merken. Bei schlechter Verbindung hingegen dauert es einige Sekunden.

Die zweite Auswirkung ist ein leicht höherer Energieverbrauch beim Versenden von Inhalten. Bei sehr guter Internetverbindung werden Anhänge ein wenig langsamer übermittelt, da sie vom System gleich 2-Mal verschlüsselt werden (Ende-zu-Ende Verschlüsselung + Kanalverschlüsselung).

Außerdem solltest du noch wissen, dass bei Apple (iOS) keine Klartext-Vorschau der Nachricht in deinen Push-Benachrichtigungen angezeigt wird – nur die Anzahl der neuen Nachrichten in Hoccer. So musst du um eine Nachricht zu lesen, die App öffnen. Der Grund warum dies so ist, ist dass wir keine Ende-zu-Ende Verschlüsselung garantieren könnten, wenn ein Ende unseren Code nicht benutzen kann, in diesem Falle das „Benachrichtigungssystem“ von iOS.

Wir hoffen, dass auch Apple es irgendwann möglich macht den eigenen Code auszuführen, wenn eine Benachrichtigung eingeht. Wenn es soweit ist, können wir diesen Service auch für Hoccer in Anspruch nehmen und unsere Benachrichtigungen in der Vorschau sichtbar machen. Bis dahin, kann man vielleicht einen großen Vorteil im Ganzen sehen: Du musst dir keine Sorgen machen, dass jemand mit einem einzigen Blick auf den Lockscreen deines Telefons deine Nachricht lesen kann.

Wo befindet sich mein Passwort und mein Login?

Passwort und Login sind „Random Strings“, die in deinem Schlüsselbund gespeichert werden. Wenn du die App löschst, werden beide gespeichert, so dass du bei Neuinstallation entscheiden kannst, ob du deine „alte“ Identität wiederherstellen möchtest.

Warum kann ich keine Freunde in der App per Telefonnummer oder Email suchen, wie bei anderen Messenger Diensten?

Wenn du die Telefonnummer oder E-Mail Adresse eines Freundes hast, kannst du diesen auch einen Einladungscode schicken. Wir sammeln oder speichern bei Hoccer keine Telefonnummern, E-mail-Adressen oder Kontaktdaten aus deinem Telefonbuch. Bei Hoccer funktioniert es wie folgt: Die Einladung wird direkt von deinem Telefon an die eingeladene Person geschickt, damit bleiben alle Daten bei dir bzw. auf deinem Endgerät und Hoccer kommt gar nicht mit diesen in Berührung.

Zusammenfassung

Unter allen vergleichbaren Anbietern von Messenger-Systemen ist Hoccer der, mit dem höchst möglichen Grad an Sicherheit und Privatsphäreschutz für Informations- und Datenaustausch auf dem Markt.

- Blog
- Company
- Presse
- Legal Notice