Sichere WhatsApp-Alternativen

Instant Messenger für Unternehmen

30.04.2021
Autor / Redakteur: Thomas Joos / Elke Witmer-Goßner

In Unternehmen ist es mittlerweile zum Alltag geworden, dass Mitarbeiter mit Instant Messengern auch über Smartphones kommunizieren. Dabei setzen viele Anwender auf WhatsApp. Im professionellen Umfeld ist das aus Datenschutzgründen aber sehr bedenklich. Wir gehen auf Alternativen ein.

Multimedia-Messaging-Apps werden vermehrt auch für die Business-Kommunikation genutzt, auch wenn sie nicht immer datenschutzkonform sind.
(Bild: © terovesalainen - stock.adobe.com)

Wenn in Unternehmen mit Instant Messengern kommuniziert wird, kommt meistens WhatsApp zum Einsatz. Allerdings kann der Messenger nicht datenschutzkonform betrieben werden. Anwender, die personenbezogene Daten beruflich über den Messenger versenden, verletzen daher in den meisten Fällen die DSGVO. Das kann für ein Unternehmen schnell zu Problemen führen.

Es gibt aber verschiedene Alternativen, die genauso einfach in der Bedienung sind, gleichzeitig aber den Datenschutz eher im Fokus haben, als WhatsApp. Es ist natürlich problemlos möglich, mehrere Messenger parallel zu nutzen. Wer für die Kommunikation

heikler Daten auf einen sicheren Messenger wie Threema, Signal, Wire oder TeamWire setzt, kann natürlich weiterhin parallel auch WhatsApp nutzen.

Auf was sollten Unternehmen beim Einsatz von Instant Messaging achten?

Wenn Anwender im Unternehmen Sofortnachrichtendienste nutzen wollen, sollte sichergestellt sein, dass die verwendete App auch konform mit der DSGVO ist. Ansonsten riskieren Unternehmen hohe Geldstrafen. Grundsätzlich sollten Daten immer nur auf europäischen, besser deutschen Servern gespeichert werden. Die Kommunikation sollte idealerweise verschlüsselt stattfinden (Ende-zu-Ende). Bei Open-Source-Messengern wie Signal und Wire steht der Quellcode der Öffentlichkeit zur Verfügung und untersteht daher ständiger Überprüfung.

Ein Messenger sollte nicht ungefragt das lokale Adressbuch auf dem Smartphone auslesen dürfen. Denn nicht jeder Kontakt ist damit einverstanden, dass seine Daten von einem Messenger ausgelesen und in der Cloud gespeichert werden.

Telegram – Die bekannteste Alternative

Telegram gehört zu den bekanntesten Alternativen von WhatsApp. Der Messenger bietet mehr Sicherheit und Datenschutz als WhatsApp, ist für den professionellen Einsatz aber nicht wesentlich besser. Es gibt bei Telegram die Möglichkeit, private Chats zu erstellen, die vollständig verschlüsselt sind inklusive der Daten des Chats. Diese werden verschlüsselt auf den Endgeräten gespeichert. Alle anderen Chats speichert Telegram in der Cloud. Datenschutztechnisch ist das sehr bedenklich, da Anwender nicht kontrollieren können, auf welchen Servern und in welchem Land die Daten gespeichert werden. Im professionellen Einsatz sollte Telegram nicht genutzt werden, da die Datenspeicherung und Verschlüsselung nicht ideal sind.

Signal – mit besonderer Empfehlung

Signal gehört sicherlich zu den bekanntesten Messengern, wenn es um die Sicherheit geht. Elon Musk und Edward Snowden empfehlen beide den Einsatz des Messengers. Signal ist Open Source. Und Signal verschlüsselt generell die komplette Kommunikation und alle Daten. Der Dienst nutzt zwar die gleiche Verschlüsselung wie WhatsApp – entwickelt wurde diese von Signal-Programmierer. Allerdings ist nur bei Signal auch nachvollziehbar, dass keine nachträglichen Veränderungen durchgeführt wurden, was

bei WhatsApp nicht so ist. Signal ist ein Messenger, dessen Schwerpunkt auf maximaler Sicherheit liegt. Allerdings muss auch hier darauf hingewiesen werden, dass der Serverstandort der Signal-Server nicht in Europa ist, der Datenschutz also nicht garantiert werden kann.

Threema – kostenpflichtig, aber sicher

Neben Signal gehört Threema gewiss zu den Messengern für Unternehmen, die am sichersten sind. Die Hersteller kommen aus der Schweiz und der Messenger hat einen guten Ruf, wenn es um sicheren Einsatz geht. Threema kann auch ohne Telefonnummer genutzt werden. Fokus von Threema sind professionelle Anwender, da bei Threema eine Identifizierung erfolgt. Falsch verschickte Nachrichten sind mit Threema kaum möglich, da alle Benutzer mit einer ID identifiziert werden. Da Threema keinen Zugriff auf das Adressbuch des Smartphones benötigt und auch ohne Angabe einer Telefonnummer funktioniert, gehört der Messenger zu den besten, wenn es um den professionellen Einsatz geht.

Wire – Ausrichtung auf professionelle Anwender

Wie Threema auch, ist der Open Source-Messenger Wire vor allem für professionelle Anwender interessant. Hier lassen sich auch private Netzwerke nutzen, in denen Anwender untereinander kommunizieren. Natürlich ist Wire Ende-zu-Ende verschlüsselt. Für Unternehmensanwender besteht die Möglichkeit, die Geräte in einem Wire-Netzwerk gegeneinander zu verifizieren. Wire nutzt für Nachrichten immer neue Schlüssel, sodass jede Nachricht erneut gesichert wird. Da Wire Open Source ist, kann der Quellcode jederzeit überprüft und auf Schwachstellen untersucht werden. Wie bei Threema, stehen auch bei Wire die Server in der Schweiz. Das Datenschutzniveau des Messengers ist dennoch sehr hoch.

TeamWire – mobile Mitarbeiter mit deutschem Messenger anbinden

Wie Wire und Threeam hat auch TeamWire eher professionelle Anwender im Fokus. Viele Behörden nutzen den Messenger teilweise. TeamWire ist laut eigenen Angaben vollständig konform zur DSGVO. Kunden haben Datenhoheit. Das heißt Anwender können selbst bestimmen, welche Daten wo und wie lange gespeichert werden. Dazu kommen bei TeamWire auch zentrale Einstellungsmöglichkeiten für Sicherheit, Kennwörter und andere Bereiche. Administratoren geben Einstellungen vor, die auf den Clients automatisch umgesetzt werden.

Auch das automatische Löschen oder Archivieren von Daten kann mit TeamWire gesteuert werden. Die Daten speichert der Messenger in deutschen Rechenzentren. Generell ist es möglich, auch einen eigenen Server bei TeamWire zu buchen. Da TeamWire auf professionelle Kommunikation ausgerichtet ist, sind nicht nur Datenschutz und Sicherheit wichtig, sondern auch Funktionen, die berufliche Anwender benötigen. TeamWire bietet dazu zum Beispiel verschiedene Nachrichtentypen, wie Alarmierungen (rot), Ankündigungen (grün) und Notizen (gelb). Wenn Nachrichten farblich hervorgehoben werden, können Anwender gezielter auf wichtige Nachrichten reagieren.

Rocket Chat – Instant Messaging selbst hosten

Wer auf den Dienst Rocket Chat setzt, kann die notwendige Backends selbst bereitstellen. Rocket Chat kann auch ohne Client-Anwendung über den Browser genutzt werden. Es stehen aber auch Apps zur Verfügung. Bezüglich der Sicherheit bietet der Messenger alle Funktionen, die von einem sicheren Messenger erwartet werden. Der größte Vorteil besteht eben darin, dass ein eigener Server betrieben werden kann.

(ID:47358913)

ÜBER DEN AUTOR

Thomas Joos

Freiberuflicher Autor und Journalist

WEITERE ARTIKEL DES AUTORS

OpenWRT, Freetz, ownCloud, NextCloud und Fritz!OS

So bauen Sie eine Private Cloud mit der AVM Fritz!Box auf