5 Gründe, warum Sie WhatsApp im Homeoffice unter keinen Umständen nutzen sollten

WhatsApp ist der unangefochtene Marktführer im Bereich der Messenger-Apps. Im Februar 2020 meldete WhatsApp rund 2 Milliarden aktive Nutzer. Somit hat fast jeder dritte Erdbewohner die kostenlose Chat-Software auf seinem Apple- oder Android-Smartphone installiert. Während der Corona-Krise wurde vielfach bekannt, dass einige Arbeitgeber, offizielle Stellen und Einrichtungen wie z.B. Schulen den Einsatz des Messengers empfehlen. Nicht zuletzt deshalb fragen sich weiterhin viele Menschen, ob sie WhatsApp im Homeoffice, in der Schule und auch privat einsetzen können. Aus folgenden Gründen, die sowohl für Apple als auch für Android gelten, raten wir eindringlich vom Einsatz ab:

1. Beim Verwenden von WhatsApp werden direkt zu Beginn im Telefonbuch gespeicherte Kontaktdaten abgegriffen und an WhatsApp- bzw. Facebook-Server gesendet werden. Dies geschieht selbst mit Adressbuchkontakten, die kein WhatsApp nutzen. Dieses systemische Problem führt zu einem klaren DSGVO-Verstoß, denn die rechtlichen Vorgaben erfordern das Einverständnis jeder betroffenen Person und können so zu Strafen und Abmahnungen führen.

2. Die Nutzungsbestimmungen von WhatsApp besagen, dass die App ausschließlich zu privaten Zwecken verwendet werden darf. Die gewerbliche Nutzung wird ausdrücklich untersagt und stellt somit einen Lizenzverstoß dar.

3. Sowohl die Datenschutzerklärung als auch die Nutzungsbedingungen kollidieren in vielerlei Hinsicht mit der gegebenen Rechtssituation. Problematisch: Nicht die App-Betreiber selbst machen sich strafbar, sondern die Nutzer – zum Beispiel durch die passive Weitergabe von Kontaktdaten, die eine explizite Einwilligung der betroffenen Person erfordert.

4. WhatsApp sammelt die Metadaten zum Nutzungsverhalten seiner Anwender und kann dafür Serververbindungen in die USA, Irland, Niederlande, Deutschland, Frankreich, Finnland und Mexiko aufbauen.

5. Die Übernahme von WhatsApp durch Facebook vor einigen Jahren hat dazu geführt, dass Facebook die Daten der WhatsApp-Nutzer erhält (u.a. auch die Telefonnummer), selbst wenn diese kein Facebook Profil besitzen. Dies ist von Facebook so gewollt und laut Datenschutzrichtlinie bestätigt, denn so können auch aus „Nicht-Facebook-Usern“ Kontaktnetzwerke erstellt werden. Die Adressbucheinträge liefern Facebook die Informationen darüber, wer wen kennt. Der soziale Graph der Nutzer wird also auch ohne Facebook-Anmeldung transparent – und das ohne Wissen und Einverständnis der Nutzer. Durch das Entfernen eines entsprechenden Häkchens in der Datenschutzerklärung soll die Weitergabe angeblich verhindert werden. Allerdings stellt allein der Opt-Out-Vorgang einen weiteren Verstoß gegen die EU-DSGVO dar.

Als positiv ist lediglich die „Ende-zu-Ende-Verschlüsselung“ hervorzuheben (für dessen Implementierung übrigens der Entwickler des Signal-Messengers engagiert wurde). Durch diese Art der Verschlüsselung ist es nahezu unmöglich, den Schriftverkehr als Außenstehender mitzulesen, ohne Zugriff auf eines der kommunizierenden Geräte zu haben. Dieses Sicherheitsfeature stellt WhatsApp in seiner Kommunikation gern nach vorn um die oben genannten Punkte zu überspielen, ohne jedoch darauf hinzuweisen, dass Facebook durchaus Zugriff auf den Endpunkt hat, denn der Rest des Messengers ist nicht Open Source.

Im Januar 2018 hat WhatsApp eine Business-Variante seiner App veröffentlicht. Laut offizieller Beschreibung ist WhatsApp Business in erster Linie für kleine Unternehmen gedacht. Die versendeten Nachrichten bei WhatsApp Business werden zwar ebenfalls durch die „Ende-zu-Ende-Verschlüsselung“ geschützt, doch sollten sich Unternehmen (wie auch Privatpersonen) im Klaren sein, dass sie die Rechte der übermittelten Inhalte an WhatsApp abtreten. Auch das grundlegende, systemische Problem der initialen und ungefragten Übermittlung der Adressbuch-Kontakte auf die amerikanischen WhatsApp-Server besteht auch in der Business-Version. Dies stellt weiterhin einen klaren Verstoß gegen das Bundesdatenschutzgesetz und die Europäische Datenschutzgrundverordnung (EU-DSGVO) dar, so dass wir auch hier dringend vom Einsatz abraten.

mediaTest digital CEO Sebastian Wolters rät den Nutzern daher: „Auf dem Messenger-Markt befinden sich sowohl für Apple- als auch für Android-Geräte mittlerweile technisch sehr ausgereifte und datenschutzrechtlich saubere Alternativen zu WhatsApp. Wir empfehlen daher auf Apps wie Signal (komplett Open Source), Threema bzw. Threema Work (Verschlüsselung Open Source), Teamwire (Closed Source) oder gar einen selbstgehosteten Jabber/XMPP-Server zu setzen. Sollten Sie von Ihrem Arbeitgeber oder anderen Stellen zum Einsatz von WhatsApp verp

Über APPVISORY® by mediaTest digital

APPVISORY ist Europas führende MTD- (Mobile Threat Defense) Software. In Verbindung mit Mobile Device Management Systemen oder Stand-Alone stellt die SaaS-Lösung den Schutz sensibler Unternehmensdaten beim Einsatz mobiler Endgeräte sicher. Mithilfe von APPVISORY setzen Unternehmen ihre individuellen IT-Sicherheitsrichtlinien sowie Vorgaben laut EU-Datenschutz-grundverordnung (DSGVO) auf ihren Mitarbeitergeräten durch.

Gleichzeitig trägt APPVISORY mit seinem App-Client zur Aufklärung und Sensibilisierung der Anwender bei und fördert die Nutzung von Apps und damit die Digitalisierung und Mobilisierung von Geschäftsprozessen. mediaTest digital sichert weltweit betrieblich genutzte Smartphones und Tablets von mehreren Hundert Kunden in der Größe von drei bis 50.000 Endgeräten ab.

Dax30-Konzerne sowie zahlreiche mittelständische und kleine Unternehmen aus Wirtschaftszweigen wie Banking, Automotive, Energieversorgung, Retail oder Behörden zählen heute zu den zufriedenen Kunden. Das in Deutschland ansässige Unternehmen nutzt ausschließlich deutsche Server für das Hosting und die Entwicklung seiner Lösungen. Weiterführende Informationen zu APPVISORY finden Sie auf www.appvisory.com.

APPVISORY®

Pressekontakt

Karina Quentin | Marketing Managerin

press@appvisory.com
Telefon +49 (0)511 20280048
Fax +49 (0)511 35 39 94-12