Fünf Gründe, warum der berufliche Einsatz von WhatsApp keine gute Idee ist

Die Nutzung des Messenger-Dienstes WhatsApp für die berufliche Kommunikation birgt einige Risiken, über die Arbeitgeber und Arbeitgeberinnen Bescheid wissen sollten.

Von Martin Jäger

Kennen Sie folgenden Fall? Die Kollegin hat wieder den Klarnamen der Patientin im WhatsApp Chat verwendet und ein Bild mit sensiblen Daten versendet? Dabei besteht bereits ein Datenschutzverstoß. Obwohl Sie eine Betriebsvereinbarung zum Einsatz von WhatsApp haben, tritt so etwas immer wieder auf. In diesem Artikel erfahren Sie, warum WhatsApp im Arbeitsalltag nichts verloren hat und weshalb Ihnen auch keine Betriebsvereinbarung hilft, den Schaden zu verhindern.

Seit Jahren sieht sich der zu Meta (ehemals Facebook) gehörende Messenger-Dienst WhatsApp herber Kritik ausgesetzt. Zahlreiche Expert:innen bemängeln mangelnde Datenschutzbestimmungen, intransparente Geschäftsbedingungen und immer häufiger auftretende Datenlecks. Und trotz der wachsenden Kritik wird WhatsApp weltweit von über zwei Milliarden Menschen im privaten und beruflichen Alltag genutzt. Dabei kann WhatsApp vor allem im beruflichen Kontext zu weitreichenden Komplikationen für die jeweiligen Unternehmen führen. Dieser Beitrag wird aufzeigen, welche Gefahren bei der Nutzung von WhatsApp – im Übrigen auch auch bei der Nutzung anderer gängiger Messenger – für Sie bestehen und auf welche Alternativen sie stattdessen zurückgreifen können.

Grund #1: Mangelnde Kontrolle über Daten und Nutzer
WhatsApp speichert die Daten von Chats inklusive der versendeten Dateien lokal auf den Handys der Nutzer. Das bedeutet, Sie verlieren jegliche Kontrolle über diese Daten. Stellen Sie sich beispielsweise vor, eine Mitarbeiter:in verlässt Ihr Unternehmen. Mit WhatsApp haben Sie keine Möglichkeit ältere Informationen für diese Person zu blockieren oder zu löschen. Was Sie per (Gruppen-)Chat versendet haben, ist für immer im Besitz des einzelnen Nutzers und Sie können nicht kontrollieren, ob die Daten gelöscht oder im schlimmsten Fall an Dritte weitergeleitet wurden. Des Weiteren gibt es keine Funktion zur Kontrolle, welche Gruppen und Chats erstellt und welche Informationen dort ohne Ihr Wissen ausgetauscht werden. Das führt ebenfalls zu einem eklatanten Datenschutzrisiko. Hier hilft auch keine Betriebsvereinbarung oder Richtlinie, denn am Ende sind Sie als verantwortliche Person für die Einhaltung der Datenschutzanforderungen zuständig. Es besteht ein erhebliches finanzielles Risiko für Ihr Unternehmen, denn die Bußgelder sind enorm.

Grund #2: Man kann WhatsApp in der Praxis nicht datenschutzkonform einsetzen
Sie brauchen die Kontrolle nicht, weil Sie allen Beschäftigten blind vertrauen können? Niemand verlässt das Unternehmen und es werden nie persönliche und sensible Daten über WhatsApp geteilt? Das halten wir schon für sehr selten bis unmöglich und selbst in diesem Fall ist WhatsApp in der Praxis nicht datenschutzkonform einsetzbar.

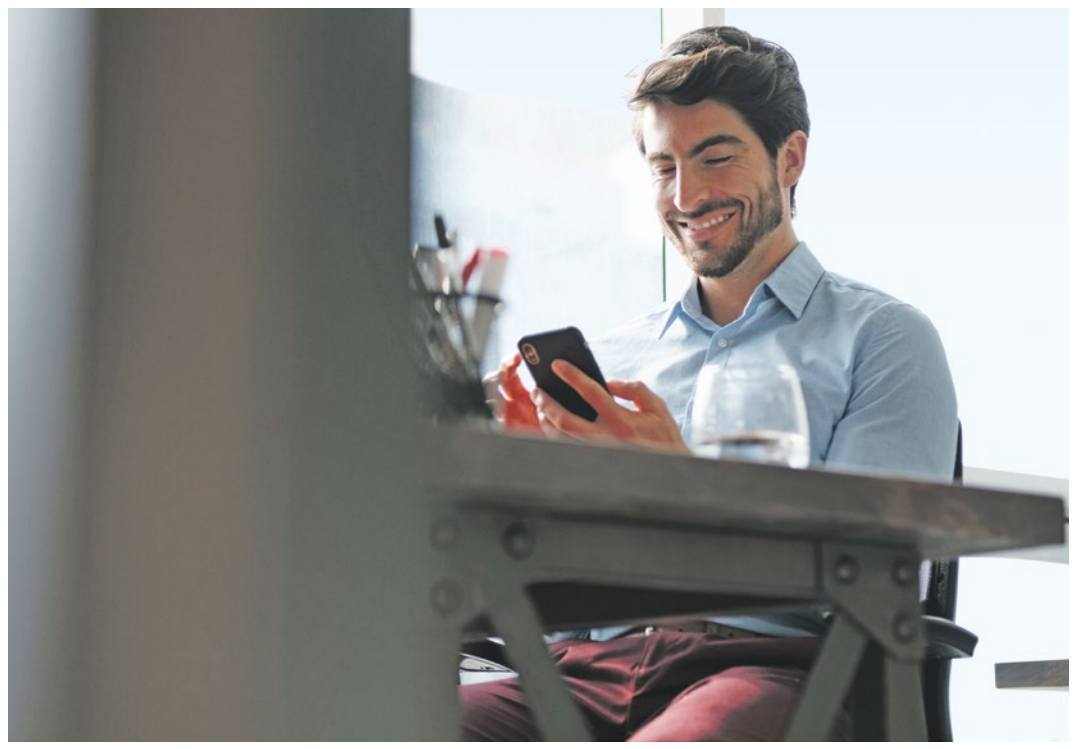
Nur einige praktische Beispiele und deren Auswirkungen:

- Es wird schnell ein Foto einer zerbrochenen Vase aufgenommen und verschickt. Im Hintergrund ist durch den Zoom die nächste Medikamentenbestellung sichtbar.
- Eine Kollegin wechselt den Telefonanbieter und die alte Nummer wird neu vergeben. Plötzlich ist eine unbekannte Person in der Gruppe, ohne dass Sie es bemerken und obwohl niemand eine böse Absicht verfolgt hat, erhält diese Person unkontrolliert Nachrichten.
- Ein Beitrag wird als unangemessen an WhatsApp gemeldet. Nun wird der Inhalt an eine Dritte Partei zur Prüfung weitergegeben und Sie verlieren jegliche Kontrolle über diese Inhalte. WhatsApp selbst weist ausdrücklich daraufhin, dass die letzten fünf Nachrichten des Kontakts oder der Gruppe nach der Meldung mit WhatsApp geteilt werden.
- Nutzt eine Kolleg:in bereits privat kein WhatsApp ist die Person von der Kommunikation abgeschnitten oder wird zur Nutzung gezwungen.

Grund #3: Chaotische Chats und verlorene Informationen
Wir stehen ständig im Austausch mit Praktikern aus der Pflege. Eines der häufigsten Probleme mit Messengern, von dem wir hören – Leute fangen an zu "chatten". Das ist auch nicht verwunderlich, denn genau dafür haben die Anbieter ihre Software optimiert. Allerdings führt es dazu, dass in einer Flut von unrelevanten Informationen die wichtigen Informationen untergehen. Es passiert einfach so viel auf einmal und ohne Struktur, dass die Benachrichtigung nicht mehr ernst genommen wird.

Außerdem ist es später nicht nachvollziehbar und ebenso wenig dokumentiert, wann, was und von wem kommuniziert wurde. Das ist schon für die internen Abläufe schwierig und führt zu unnötigem Hin und Her. Erst recht problematisch wird es, wenn bei der nächsten MDK-Prüfung ein Nachweis geführt werden soll oder ein Qualitätsmanagement-Audit bevorsteht. Setzen Sie daher auf eine getrennte Software für Ihre berufliche Kommunikation, die für Ihren Anwendungsfall optimiert wurde.

> WhatsApp ist in der Praxis nicht datenschutzkonform einsetzbar.



Wer WhatsApp beruflich nutzt, verliert auch die Kontrolle über sensible Daten. Foto: Adobe Stock/engagestock

Grund #4: Privat- von Berufsleben trennen
Neben den bisher genannten rechtlichen Problemen, dürfen auch die privaten Aspekte nicht außer Acht gelassen werden. Denn eine ständige Erreichbarkeit führt in vielen Fällen zu Stress und im schlimmsten Fall zu Burn-out, der vermieden werden kann. Die Beschäftigten sind „always on", da es keine Möglichkeit gibt, sich vom beruflichen Teil der Kommunikation abzumelden. Selbst kurze Nachrichten, die Beschäftigte außer Dienst erreichen, werden auf Dauer zur Belastung und lassen sich aufgrund verschiedener Schichten und Arbeitszeiten auch nicht vermeiden.

Zudem kann es vorkommen, dass private Nachrichten und Bilder versehentlich an die falschen Personen oder Gruppen weitergeleitet werden. Im besten Fall führt dies zu Verwirrungen und im schlimmsten Fall können solche Nachrichten überaus unangenehm und unpassend sein.

Aus den genannten Gründen ist es deshalb ratsam, WhatsApp nicht für den beruflichen Gebrauch zu nutzen.

Grund #5: Datenschutzbestimmungen und Standort in den USA
Das zu Meta (ehemals Facebook) gehörende Unternehmen WhatsApp hat seinen Sitz in den USA und stellt seine Services von dort bereit. Entsprechend sind auch die Nutzungsbedingungen sowie das Teilen von Meta Daten aus Perspektive eines amerikanischen Konzerns aufgebaut - und wer liest die Nutzungsbedingungen wirklich? Wussten Sie zum Beispiel, dass noch nicht zugestellte Nachrichten bis zu 30 Tage auf den Servern von WhatsApp gespeichert werden? Das steht so in den Nutzungsbedingungen. Ohne Erklärung, wo diese Server stehen, welche Anforderungen eingehalten werden und Ähnliches. Sie können also nicht sicherstellen, dass die Daten nicht doch in den USA auf einem Server von Meta landen.

Wenn Sie WhatsApp nutzen, geben Sie zusätzlich Dritten Zugriff auf alle Kontakte, die in Ihrem Adressbuch gespeichert sind. Es geht noch weiter: Sie stimmen sogar ausdrücklich zu, dass WhatsApp auf Ihre „Kontaktlisten und/oder auf Ihr Adressbuch zugreifen darf, um die Nutzung des WhatsApp-Services zu gewährleisten."

Im privaten Bereich können Sie dieses Risiko selbstbestimmt tragen und akzeptieren. Für Ihr Unternehmen kann es weitreichende rechtliche und finanzielle Auswirkungen haben.

Sichere Alternative zu WhatsApp: Auf dem Markt gibt es zahlreiche Messengerdienste wie beispielsweise Signal, Telegram, Threema oder Wire, die als Alternative zu WhatsApp genutzt werden können. Viele der genannten Dienste verfügen über eine vergleichsweise höhere Datensicherheit als WhatsApp. WhatsApp sowie diese Messenger sind hervorragend für die private Kommunikation mit Freunden oder der Familie geeignet. Für den beruflichen Zweck sind sie allerdings nicht zu empfehlen.

Denn auch die genannten Alternativen sind nicht unbedingt DSGVO-konform. Darüber hinaus können Unternehmen nicht steuern, wie sich die Geschäftsbedingungen der jeweiligen Anbieter im Laufe der Zeit ändern. Daraus folgt: Möchte man eine DSGVO-konforme Kommunikation im beruflichen Kontext gewährleisten, bleibt einzig die Möglichkeit, auf Software zurückgreifen, die eigens für den beruflichen Kontext entwickelt wurde.

Der Autor ist Geschäftsführer der Kommunikationsplattform noaa.

Ein selbstbestimmtes Leben erleichtern

Musterwohnung in Hannover erprobt smartes Wohnen im Alter

Noch hat Jutta Heinrich (76) den Überblick, welche Tabletten sie wann einnehmen muss. „Doch bald werde ich mir auch so einen automatischen Tablettendosierer kaufen", sagt die Rentnerin und zeigt auf das Behältnis vor sich auf dem Tisch. Wenn die Zeit zur Einnahme gekommen ist, piepst das Gerät und gibt die jeweiligen Medikamente frei.

Diesen und dutzende andere digitale Alltagshelfer können Seniorinnen und Senioren in einer 2017 von der Stadt Hannover eingerichteten Musterwohnung ausprobieren. Zudem ist der Ort seit Frühjahr 2022 Versuchslabor für „smartes", also computerisiertes Wohnen im Alter, im Rahmen des vom Bundesfamilienministerium geförderten Projekts „Digital souverän mit Künstlicher Intelligenz" der Bundesarbeitsgemeinschaft der Seniorenorganisationen. Das Projekt soll zeigen, wie moderne Technik selbstbestimmtes Wohnen erleichtern kann, wenn die körperlichen und geistigen Kräfte abnehmen. (epd)

Mehr zu dem Projekt finden Sie hier: seniorenberatung-hannover.de/info/digitalisierung/smarte-musterwohnung-und-technikberatung

SENovation-Award 2023

Bewerbungsphase läuft

Der Demografische Wandel ist kein Zukunftsszenario, sondern Realität. Junge Gründerteams zeigen mit innovativen Konzepten Lösungswege auf. Der SENovation-Award zeichnet 2023 im sechsten Jahr Innovationen für eine alternde Gesellschaft aus. Die Bewerbungsphase läuft vom 2. Januar bis 30. Juni 2023. Finale ist dann am 13.9.2023 in Dortmund. Die beiden Gewinnerteams erhalten jeweils einen Geldpreis in Höhe von 5.000 Euro sowie individuelle Coaching-Maßnahmen. (ck)

senovation-award.de