WEB +APP
Besser surfen, mehr erleben

Von **Valerie Hagmann**

Das WhatsApp-Dilemma

Obwohl WhatsApp Daten europäischer Nutzer nicht für Werbezwecke an Facebook weitergeben darf, findet ein Datenaustausch längst statt. Somit bezahlen wir die Nutzung des kostenlosen Messenger-Dienstes mit unseren Daten. Was Sie darüber wissen sollten und warum es besser wäre, dem Messenger den Rücken zu kehren.

Anfang Jänner ging ein erschrockenes Raunen durch die Reihen der WhatsApp-Nutzer, das sich schnell zum medialen Empörungssturm entwickelte: Ein Pop-up-Fenster informierte beim Öffnen der App über geplante Änderungen der Nutzungsbedingungen sowie der Datenschutzrichtlinie des beliebten Messengers.

Die Änderungen erlauben dem Messenger einfach gesagt, künftig sämtliche Nutzungsdaten an andere Unternehmen der Facebook-Familie weiterzugeben und diese gezielt für Werbezwecke zu verwenden. Nachrichteninhalte sind davon ausgenommen, da diese verschlüsselt gesendet werden.

Nur mit einem Ja zu den neuen AGB kann WhatsApp in Zukunft weiterhin genutzt werden, heißt es in der Meldung. Facebook sichert sich damit die Erlaubnis der Anwender, mithilfe der erhaltenen Informationen seine Dienste, einschließlich der Produkte von Facebook-Unternehmen, „zu betreiben, bereitzustellen, zu verbessern, zu verstehen, zu individualisieren, zu unterstützen und zu vermarkten."

Vorerst kaum Änderungen für EU-Bürger

Die Ankündigung hat Fragen aufgeworfen, viele Anwender verunsichert und sie dazu bewogen, sich nach Alternativen umzusehen. Nicht etwa die öffentliche Kritik, aber der darauffolgende massive Rückgang der Nutzerzahlen dürfte WhatsApp dann bewogen haben, den Zeitpunkt des Inkrafttretens der Änderungen vom 8. Februar auf den 15. Mai 2021 nach hinten zu verschieben und in mehreren Stellungnahmen zu beschwichtigen.

Die Änderung gelte in dieser Form nicht für EU-Bürger, auch wenn man ihr am Ende zur weiteren Nutzng von WhatsApp zustimmen müsse, so das Unternehmen. Der Punkt zur Nutzung der Daten für personalisierte Werbung fehlt tatsächlich in der europäischen Version der neuen AGB, da die EU Facebook die Verwendung der Daten für zielgerichtete Werbung nicht erlaubt. Dies bestätigte auch Niamh Sweeney, WhatsApp-Policy-Direktorin für Europa, in einer Twitter-Nachricht. Ihr zufolge würde mit den neuen Nutzungsbedingungen in Europa lediglich sichergestellt, dass Unternehmen, die WhatsApp Business nutzen, mit Facebook-Tools weiterhin auf WhatsApp-Daten ihrer Kunden zugreifen können, um ihre Services adäquat anzubieten. Daten privater Anwender in Europa würden nach wie vor nicht zu Werbezwecken genutzt, so Sweeney, sondern lediglich, um das Nutzererlebnis zu verbessern.

Gratis ist nicht kostenlos

Für Privatanwender in Europa ändert sich durch die neuen AGB also vorerst nichts. Das ist aber keineswegs ein Grund zum Aufatmen. Denn dass Face-

book Daten nicht verwenden darf, heißt nicht, dass diese grundsätzlich nicht weitergegeben werden – das ist definitiv der Fall, und zwar schon seit Jahren. 2019 verhängten die US-Aufsichtsbehörden eine Milliardenstrafe über Facebook, nachdem herausgekommen war, dass die Analysefirma Cambridge Analytica Daten von rund 87 Millionen Facebook-Nutzerinnen und -Nutzern abgegriffen und mutmaßlich dazu missbraucht hatte, den US-Wahlkampf zu beeinflussen.

Auch wenn Facebook 2014 bei der WhatsApp-Übernahme den EU-Regulatoren versicherte, dass ein Datenaustausch zwischen seinen Diensten niemals vorkommen werde – eine Aussage, welche die EU zur Bedingung für ihre Zustimmung zur Übernahme machte –, wurde eine entsprechende Passage 2016 dennoch in den Messenger-Nutzungsbedingungen verankert. Für die eigentlich unerlaubte Änderung nahm Facebook 2016 eine Strafzahlung der EU-Kommission von über hundert Millionen Euro in Kauf. Das Unternehmen hatte nämlich ursprünglich behauptet, dass es niemals vorhabe, die Dienste miteinander zu verbinden; sogar dass dies technisch gar nicht möglich sei. Eine Behauptung, der die EU-Regulatoren kurzsichtigerweise Glauben geschenkt hatten. Dass Facebook nicht aus reiner Nächstenliebe 19 Milliarden US-Dollar für WhatsApp hingeblättert hat, sollte eigentlich Hinweis genug gewesen sein.

Außerhalb Europas werden Nutzerdaten schon längst auch zu Werbezwecken eingesetzt. Dafür gab es bisher ein Opt-out – mit der Änderung wird die Zustimmung allerdings zum Muss. Der Facebook-Konzern lebt eben davon, Nutzerdaten zu Geld zu machen. Jeder Kommentar, jeder Like, jedes gespeicherte Bild gibt Aufschluss darüber, was uns wichtig ist – und zwar Dritten gegenüber! Mit wem wir wann und wie oft chatten, sagt viel über unsere Beziehungen aus. Miteinander verknüpft lassen sich so sehr genaue Profile erstellen. Mit der Änderung stellt Facebook die Weichen dafür, seine Dienste noch näher zusammenzuführen und genau dies zu erreichen – und für kommerzielle Zwecke zu nutzen. >

Vollbild

S-AUTTERSTOCK

Abseits von Datenschutzbedenken bedeuten stark personalisierte Inhalte auch, dass wir über soziale Medien nur mehr ein recht verzerrtes Bild der Realität gezeigt bekommen. Jeder von uns sitzt, auch jetzt schon, in der eigenen, individuell angepassten Interessenblase aus Anzeigen und Content-Vorschlägen fest.

Warum WhatsApp problematisch ist und bleibt

WhatsApp ist, gemessen an der Zahl der Downloads, der meistgenutzte Messenger-Dienst der Welt und sogar eine der beliebtesten Apps überhaupt. Im Februar 2020 wurde die Zwei-Milliarden-Downloads-Marke geknackt. Zum Erfolgsrezept gehören die simple und intuitive Handhabung sowie die vielseitigen Nachrichten-Features und nicht zuletzt die große Nutzerbasis. Mit WhatsApp Business hat das Unternehmen auch eine eigenständige App für Kleinunternehmer entwickelt, mit welcher diese mit ihren Kunden in Kontakt treten können.

Nicht erst seit der Übernahme durch Facebook wird die Datensicherheit von WhatsApp aber immer wieder stark angezweifelt. Seit der beschriebenen, verbotenerweise durchgeführten AGB-Änderung 2016 werden die Telefonnummer, einige Geräteinformationen sowie Informationen über das Nutzungsverhalten an Facebook weitergegeben. Das sei nötig, um „die Sicherheit und Integrität aller Produkte von Facebook-Unternehmen zu fördern", wie sich nachlesen lässt. Diese einigermaßen vage Formulierung meint unter anderem Schutz vor Missbrauch, Spam oder Rechtsverstößen. Zudem werden Daten weitergegeben, um die Dienste korrekt zu betreiben, zu verbessern und zu vermarkten.

Dass das Unternehmen im Falle von Kritik immer wieder auf dieselben Argumente pocht, in seinen AGB allerdings oft sehr vage oder widersprüchlich formuliert, scheint Methode zu haben. Die Formulierungen lassen viel zu oft sehr viel Raum für Interpretation – sowohl für das Unternehmen als auch für die Nutzer. Es entsteht der Eindruck, dass WhatsApp und vor allem die Konzernmutter Facebook

Jeder Kommentar, jeder Like, jedes gespeicherte Bild gibt Aufschluss darüber, was uns wichtig ist – und zwar Dritten gegenüber!

nicht allzu viel Interesse daran haben, den Nutzern Klarheit über die Verwendung ihrer Daten zu verschaffen. Die gültigen AGB können bereits so ausgelegt werden, dass die Daten der WhatsApp-Gemeinde innerhalb des Konzerns ziemlich uneingeschränkt herumgereicht werden dürfen.

Große Unternehmen sind nicht an sich schädlich. Doch eine große Anwenderbasis bedeutet viele Daten, und das heißt unterm Strich konzentrierte Marktmacht und eine stärkere Tendenz zu problematischen Strukturen, die dann globale Auswirkungen haben können. Welche Ausmaße das annehmen kann, zeigte das Pandemie-Jahr 2020 recht deutlich mit Massen an unregulierten Falschinformationen auf sozialen Plattformen und den dazugehörigen Gruppen, die aufgrund ihrer einschlägigen Interessen dann auch nur mehr ähnlich problematische Inhalte sowie Gleichgesinnte als Kontakte vorgeschlagen bekommen und ihre Filterblase für die Realität halten.

Aktuell läuft übrigens eine Klage der US-Regierung gegen den Facebook-Konzern. Der Vorwurf lautet: Aufbau eines illegalen Monopols durch die Übernahmen von Instagram und WhatsApp. Die Europäische Union hat in dieser Hinsicht derzeit keine Bedenken.

Dass viele Menschen sich derlei Dinge sehr wohl bewusst sind, mangels populärer Alternativen aber bisher bei dem Dienst geblieben sind, legt unter anderem der Massen-Exodus der WhatsApp-User nahe, welcher auf die Ankündigung der AGB-Änderungen folgte. Millionenfach kehrten sie der Nachrichten-App den Rücken.

Wohin wechseln?

An Alternativen zu WhatsApp mangelt es nicht, dennoch scheitern Wechselwillige an der Tatsache, dass die Nutzerbasis aller anderen Messenger-Apps um einiges kleiner ist als die der Facebook-Tochter – oder es zumindest bis vor kurzem war. Letztendlich bringt ein noch so sicherer Messenger wenig, wenn Freunde, Familie und Kollegen ihn nicht ebenfalls nutzen. Die wenigsten Anwender verweigern sich deshalb konsequent den Kommunikationskanälen des Facebook-Konzerns, wenn das angesichts der Datenschutz-Problematik auch ein erstrebenswerter Ansatz ist. So viele Unterhaltungen wie möglich auf andere, besser geschützte Kanäle zu verlegen, ist auf jeden Fall empfehlenswert, auch wenn man WhatsApp nicht gleich komplett hinter sich lässt.

Als Alternativen sind Dienste wie Threema, Telegram, Wire und allen voran Signal in aller Munde. Sie nutzen die gleiche technische Grundlage für die Verschlüsselung ihrer Nachrichten, sammeln und verwenden allerdings nicht in diesem kolossalen Ausmaß Metadaten oder gehen sorgsamer damit um – und sind vor allem nicht mit großen Internetkonzernen verknüpft, welche diese weiterverwenden könnten.

Viele dieser Apps, die in erster Linie ihren Nutzern verpflichtet sind, konzentrieren sich im Gegenteil sogar auf Features zum Datenschutz. Das bedeutet, dass die von ihnen gesammelten Daten idealerweise nicht auf die jeweiligen Nutzer zurückgeführt werden können, wie das bei WhatsApp der Fall ist.

Welche App ist nun die richtige? Das lässt sich pauschal nicht sagen. Vor der Wahl einer geeigneten App zahlt es sich immer aus, das Kleingedruckte zu lesen und ein paar wesentliche Fragen zu klären. Im Fall von Messenger-Diensten sollten Interessierte also die Informationen im App-Store unter die Lupe nehmen. Welche Berechtigungen verlangt der Dienst am Smartphone, welche Daten werden wie und wie lange gespeichert, wie finanziert sich die App, wie sieht es mit Verschlüsse-

FOTOS: 123RF.COM

Kleines Sicherheitsglossar

Ende-zu-Ende-Verschlüsselung: Die Nachricht wird am Gerät des Senders verschlüsselt, nur das empfangende Gerät kann sie entschlüsseln. Der Gesprächsverlauf wird nicht auf Servern gespeichert. Das bedeutet, dass die Inhalte nur von den Gesprächspartnern eingesehen werden können. Nicht einmal der Servicebetreiber hat Einblick in die Inhalte.

Metadaten: Darunter versteht man verschiedenste Daten, die Aussagen über das Nutzungsverhalten einer App zulassen. Mit wem wird wann, wie oft und wie lange kommuniziert? Welche Arten von Daten werden wie oft und wem geschickt? Wann und wie lange sind Nutzer online? Bei nicht verschlüsselten Messengern können Dritte relativ einfach auf diese Daten zugreifen und ein aussagekräftiges Aktivitätenprotokoll erstellen, welches dann für zielgerichtete Werbung genutzt werden kann. So offenbaren sich Details über Beziehungen zwischen Personen, Vorlieben und über längere Zeiträume ein ziemlich genaues Persönlichkeitsprofil der Person, welches monetarisiert werden könnte.

Open-Source-Software: Jede Person mit dem nötigen technischen Verständnis kann den Code der quelloffenen Software einsehen, überprüfen und verbessern.

lung und Datenschutz aus? In welchem Land stehen die Server, welchen Datenschutzgesetzen unterliegen sie? Wesentlich ist auch, ob für die Anmeldung E-Mail-Adresse oder Telefonnummer benötigt werden (Signal, Telegram, WhatsApp) oder der Messenger gar eine Nutzer-ID zur Identifikation vergibt (Threema, Wire), sodass die Angabe von Kontaktdaten wegfällt.

Die meistgenannten Alternativen stellen wir kurz vor.

Große Vorsicht bei Telegram

Telegram durfte sich über einen enormen Zuwachs freuen, rund 500 Millionen Menschen nutzen den Messenger bereits. Den Dienst können wir allerdings nicht als sichere Alternative empfehlen. In gewisser Weise ist er noch unsicherer als WhatsApp. Chats werden standardmäßig nicht ausreichend verschlüsselt und basieren auf einem für Außenstehende nicht einsehbaren Code. Wie genau die Software arbeitet, ist also nicht ersichtlich. Außerdem speichert Telegram sämtliche Eingaben auf seinen Cloud-Servern. Dort sind sie für Dritte, die sich Zugang verschaffen, leichte Beute. Der Serverstandort ist nicht bekannt – das heißt, es ist auch nicht klar, welchen Datenschutzgesetzen er unterliegt.

Die Möglichkeit, Gruppenchats mit bis zu 200.000 Teilnehmern zu erstellen, ist an sich beeindruckend. Damit avanciert der Dienst aber immer mehr zur Plattform für Verschwörungstheoretiker und rechtsextreme Gruppierungen, die von anderen Plattformen ausgeschlossen wurden und nun über Messenger ihre zweifelhaften Meinungen verbreiten.

Urgestein Threema

Der Messenger aus der Schweiz war einer der Vorreiter in Sachen Sicherheit und ist seit 2012 im Geschäft. Der Quellcode ist seit kurzem offen, sämtliche Kommunikation ist Ende-zu-Ende-verschlüsselt. In Chats können Fotos, Videos und der Standort verschickt werden, auch einen Desktop-Client gibt es. Einzelne Unterhaltungen lassen sich optional mit einem PIN-Code schützen. Mit Metadaten ist der Dienst sehr sparsam. Für die Anmeldung ist deshalb keine Angabe der Telefonnummer erforderlich, stattdessen wird dem Nutzer eine zufällige Threema-ID zugeordnet. Das bedeutet, der Messenger kann tatsächlich anonym genutzt werden. Threema ist im Gegensatz zu den anderen besprochenen Messenger-Apps nicht kostenlos, mit rund vier Euro aber absolut erschwinglich.

Business-Lösung Wire

Die deutsch-schweizerische Nachrichten-App ist – wie Threema – vollständig Ende-zu-Ende-verschlüsselt und Open Source. Im Vergleich zu den anderen vorgestellten Apps ist die Nutzerbasis noch kleiner, denn Wire zielt auf den Einsatz im professionellen Kontext ab und bietet dafür auch Pro-Versionen. Mit Clients für Mac und Windows lässt sich der Dienst ohne Telefonnummer und notfalls auch ohne Smartphone nutzen. Registrieren kann man sich stattdessen per E-Mail.

Empfehlung der Redaktion: Signal

Was vor Jahren schon Whistleblower und Ex-CIA-Mitarbeiter Edward Snowden empfahl, wurde zuletzt von Tesla-Gründer Elon Musk bestärkt: „Nutzt Signal!" Von dieser prominenten Unterstützung profitierte der Dienst in den letzten Wochen enorm. Über 40 Millionen neuer Nutzer rannten ihm regelrecht die Türen ein. Mitte Jänner war der Andrang so groß, dass die Signal-Server unter den Neuanmeldungen über ein paar Tage hinweg mehrmals in die Knie gingen.

Im Gegensatz zu WhatsApp finanziert sich Signal über eine gemeinnützige Stiftung und ist daher nicht darauf angewiesen, durch seine Nutzer Geld zu lukrieren. Alle Chats werden standardmäßig verschlüsselt.

Die Bedienoberfläche ähnelt der von WhatsApp, daher ist der Umstieg nicht allzu schwierig. Der Dienst bietet Video-Telefonie, seit neuestem auch für Gruppen, hat einen Desktop-Client und bietet selbstzerstörende Nachrichten. Neue Features werden nur dann zugelassen, wenn sicher ist, dass darüber keine Daten gesammelt werden. Ein weiterer Pluspunkt: Der Code ist Open Source, kann also von jedem eingesehen werden. Bei der Installation fragt Signal übrigens zwar nach Zugriff auf das Adressbuch, dabei werden aber keine Daten ans Unternehmen weitergegeben, welche Rückschlüsse auf den Nutzer zulassen. Derzeit läuft die Registrierung noch über die Telefonnummer, bald schon soll es aber auch ohne gehen. <<

FOTOS: HERSTELLER