Foto: skyla80 Shutterstock.com

Datenschutz: WhatsApp

Chat mit Risiko

WhatsApp ist eines der unsichersten Online-Netzwerke überhaupt. Das Recht auf Datenschutz bleibt bei diesem Messenger komplett auf der Strecke.

Vor zwei bis drei Jahren hat sich unter Jugendlichen die Ansicht durchgesetzt: Facebook ist „out"; WhatsApp ist die neue Anwendung, über die man sich austauscht. Bald begannen auch immer mehr Erwachsene, den Dienst zu nutzen. Mittlerweile sind es rund 700 Millionen User weltweit, die jeden Tag rund 30 Milliarden Nachrichten, 700 Millionen Fotos und 100 Millionen Videos teilen. In Österreich wird die Nutzer-Zahl auf über eine Million geschätzt. WhatsApp, so heißt es, hat SMS und MMS so gut wie ersetzt. Klingt nach einer sinnvollen Dienstleistung, die noch dazu kostenlos ist. Sie bringt nur ein großes Problem mit sich: Um die Datensicherheit ist es bei WhatsApp eher schlecht bestellt – noch schlechter als bei vergleichbaren Diensten.

Her mit allen Daten!

Das beginnt schon bei der Anmeldung. Wer die App auf sein Smartphone laden will, muss zuerst eine Reihe an fragwürdigen Zugeständnissen machen. Denn der Messenger fordert schon vor der Installation eine Einwilligung für den Zugriff auf App-Käufe, den Geräte- und App-Verlauf, die Identität des Handybesitzers, seine Kontakte, seinen Standort, seine SMS, Fotos, Medien und andere Dateien; auf seine Kamera und sein Mikrofon, seine WLAN-Verbindungsinfos und seine Geräte-ID sowie die Anrufinformationen. Sprich: Der Dienst lässt sich den Zugriff auf alles bewilligen und kann sich schon bei der Installation alle Daten auf seine Server ziehen – was generell, vor allem aber bei den Kontakten, bedenklich ist. Denn das Unternehmen erhält dadurch Informationen über Menschen, die mit dem Dienst nichts zu tun haben und auch nie ihr Einverständnis zu einem Zugriff gegeben haben.
Erst wenn die Einwilligung dazu erteilt ist, gelangt der User auf die Willkommens-Seite, wo er aufgefordert wird, den Allgemeinen Geschäftsbedingungen zuzustimmen und fortzufahren. Den Link zu den AGB klicken die wenigsten überhaupt an, geschweige denn, dass sie den zwölf A4-Seiten langen Text durchlesen oder zumindest überfliegen. Dabei erfährt der Kunde in den AGB, worauf er sich einlässt. Allerdings ist eine sprachliche Hürde zu überwinden, denn der Text steht nur auf Englisch zur Verfügung. In Deutschland wurde das bereits für gesetzwidrig erklärt, nur hat das Unternehmen bis dato nicht reagiert und noch keine deutsche Fassung herausgebracht. Laut österreichischem Recht verhält es sich ähnlich. Sobald eine App ihre Inhalte in deutscher Sprache anbietet, muss sie eigentlich auch ihre AGB übersetzen.

Die Liste der Klauseln hat es jedenfalls in sich: WhatsApp ...

- kann seine AGB jederzeit ändern, und es liegt in der Verantwortung des Nutzers, sich auf den neuesten Stand zu bringen.
- ist für Personen unter 16 Jahren nicht vorgesehen, heißt es in den AGB. Nur: WhatsApp prüft das Alter der Nutzer nicht.
- sichert sich die Rechte an den Daten und Inhalten der Nutzer.
- übernimmt keine Garantie dafür, dass Inhalte vertraulich behandelt und sicher übertragen werden.
- behält sich vor, die Userdaten mit Dritten zu teilen, „wenn es für die Nutzung, Pflege und Verbesserung des Services nötig ist".

Liest Facebook mit?

In den AGB sichert sich das Unternehmen also den Zugriff auf die Daten seiner Nutzer. Wobei kein User genau weiß, was das Unternehmen damit anstellt und wie lange es sie speichert. Zwar gibt WhatsApp selbst bekannt, dass Daten nur so lange gespeichert werden, bis sie den Empfänger erreicht haben, und auch das nur für maximal 30 Tage. Dass dies wirklich der Fall ist, hat aber noch niemand nachweisen können.
Dabei spielt auch der Umstand mit, dass der Social-Media-Riese Facebook im Vorjahr

Foto: Yurchyks / Shutterstock.com Montage: Erwin Haberl

Bisher erschienen:
Google und der Datenschutz, KONSUMENT 1/2015, Facebook und der Datenschutz, KONSUMENT 2/2015, Amazon und der Datenschutz, KONSUMENT 3/2015

WhatsApp übernommen und sich dadurch die absolute Vormachtstellung unter den Online-Netzwerken gesichert hat. Damals versprachen die Chefs der beiden Firmen, dass Kundendaten nicht zusammengelegt würden. Auch jüngst hieß es wieder, dass es dabei bleiben solle. Man tausche sich nur über die Strategie aus, auch was Möglichkeiten zum Geldverdienen betreffe, erklärte ein Facebook-Manager unlängst. Und genau deswegen schenkt der aufgeklärte User der Mär von den getrennten Daten keinen Glauben. Denn mit verknüpften Daten lässt sich noch mehr Umsatz machen.

Leicht zu knacken

Auch für den Fall, dass sich Dritte unerlaubt Zugang zu den Daten verschaffen, hat sich das Unternehmen in den AGB abgesichert. Dass das durchaus passieren kann, haben in der Zwischenzeit gleich zwei Softwareentwickler bewiesen.
Der Niederländer Maikel Zweerink hat den relativ simpel anzuwendenden Dienst WhatsSpy Public entwickelt. Damit können Onlinestatus, Profilbilder, Statusnachrichten und die Datenschutzeinstellungen jedes beliebigen WhatsApp-Nutzers überwacht werden. Nicht einmal ein Hackerangriff ist dafür nötig. Es wird bloß auf die Einstellungen zugegriffen.
Und Forscher der Universität Ulm haben eine Software entwickelt, mit der der Onlinestatus eines jeden Users ohne dessen Wissen und ohne zu hacken überprüft werden kann – auch wenn dieser den sogenannten Zeitstempel („zuletzt online") deaktiviert hat. Mit diesen Daten konnten die Informatiker einen beachtlichen Einblick in den Tagesablauf des einzelnen Nutzers gewinnen.

Schritte zu mehr Datensicherheit

Was kann der Nutzer gegen die Datensaugerei unternehmen? Die konsequenteste Vorgangsweise ist, das WhatsApp-Konto zu löschen (eine Anleitung hierzu gibt es z.B. auf netzwelt.de/news/121991-whatsapp-konto-loeschen-so-kuendigen-messenger.html). Doch nicht alle wagen den Schritt, zumal es sich um den meistverwendeten Messaging-Dienst handelt und sie dadurch von der Kommunikation mit ihrem Freundes- und Bekanntenkreis auf dem Kanal ausgeschlossen würden.
Dabei es gibt alternative Anbieter, die seit Bekanntwerden der Übernahme von WhatsApp durch Facebook stark aufgeholt haben. Der Dienst Line etwa verdient sein Geld nur mit dem Verkauf von Stickern. Wer viel Gebrauch von Gruppen-Chats macht, ist mit der App GroupMe gut beraten. Oder mit KakaoChat: Der Dienst arbeitet mit einer verschlüsselten Kommunikation und hat sich seine Datensicherheit ISO-zertifizieren lassen. Recht populär ist auch das Start-up Viber, und unter Datenschützern sind die Schweizer Apps Threema und MyEnigma beliebt, da sie auf komplett verschlüsselte Kommunikation setzen. Das Problem dabei: Möchte man einen solchen Dienst nutzen, muss man seine Freunde und Bekannten dazu überreden, dies ebenfalls zu tun.

Einstellungen anpassen

Wer sich für den Verbleib auf WhatsApp entschließt, der sollte zumindest seine Datenschutz-Einstellungen kontrollieren. Wenngleich diese Maßnahmen nur sehr beschränkt und in folgenden Fällen helfen: Zwei graue Häkchen signalisieren, dass eine Nachricht versandt wurde bzw. beim Empfänger angekommen ist. Die Farbänderung auf Blau gibt Auskunft darüber, dass sie gelesen wurde.
Auch das Profilbild und der Status sind Thema. Unter „Einstellungen" -> „Account" -> „Datenschutz" kann – zumindest in der Android-Version der App – die Lesebestätigung ausgeschaltet werden. Dann sieht der Chatpartner nicht, ob ich die Nachricht schon gelesen habe. Umgekehrt kann derjenige, der diese Einstellung vorgenommen hat, auch keine Bestätigungen von anderen sehen. Der „Zuletzt online"-Status kann ebenfalls unter „Datenschutz" ausgeschaltet werden, wodurch die anderen User nicht mehr sehen können, wann man WhatsApp zuletzt benutzt hat. Der Onlinestatus selbst lässt sich nicht verbergen. Beim Profilbild und dem Status kann der Nutzer indes wählen, ob diese Info für jeden, nur für seine Kontakte oder für niemanden ersichtlich ist. „Jeder" sollte dabei keinesfalls eingestellt werden.

Europäisches Verbraucherzentrum Österreich ECC-Net
www.europakonsument.at

Co-funded by the European Union

Dieser Artikel entstand im Rahmen der Tätigkeiten des Netzwerkes der Europäischen Verbraucherzentren (ECC-Net).

Obsoleszenz

Virtuelle Sollbruchstellen

Einst wurden Waschmaschinen oder TV-Geräte als Erbstücke an die nächste Generation weitergereicht. Heute führt oft bald nach Ablauf von Garantie und Gewährleistung eine Einbahnstraße direkt zur Mülldeponie. Eine Reparatur würde den Neupreis übersteigen und wird auch gar nicht mehr angeboten – von Ersatzteilen ganz zu schweigen. Kann es nicht so etwas wie den goldenen Mittelweg geben?

Gernot Schönfeldinger
gschoenfeldinger@konsument.at

Während diese Frage ungehört verhallt, hängt das Damoklesschwert der Obsoleszenz über jedem Neukauf. Viele Produkte enthalten Sollbruchstellen, mutmaßen Kunden aufgrund leidvoller Erfahrungen. Die Hersteller weisen natürlich strikt zurück, dass so etwas wie geplante Obsoleszenz existiert. Selbst für den jeglichen Hausverstand verspottenden Einbau von Verschleißteilen aus Kunststoff haben sie gute Begründungen.
Das Spiel läuft längst schon auch auf anderen Ebenen: Zwei Jahre alte Smartphones erhalten keine Sicherheitsupdates, weil die Geräte nicht mehr erzeugt werden (LG); ältere, voll funktionsfähige Computer sind nicht auf die aktuelle Version des Betriebssystems aufrüstbar, während der Hersteller jede Unterstützung für das alte einstellt (Apple); die Fehlerbehebung angesichts der Inkompatibilität eines Bildverwaltungsprogramms mit einem aktuellen Betriebssystem geschieht in der Form, dass man allen Betroffenen die neue Version des Programms verkauft (ACDSee); separat erworbenes Kartenmaterial wird mit einem konkreten Navigationsgerät verknüpft und ist nur dann auf ein anderes Gerät übertragbar, wenn das alte entsorgt wird – selbst wenn dieses funktionstüchtig ist und weitergegeben werden könnte (Garmin); die Hersteller liefern keine Treiber-Updates für wenige Jahre alte Drucker, sodass ein Computerneukauf Folgekosten nach sich zieht (Canon, HP). Eine Handvoll Beispiele für viele virtuelle Sollbruchstellen.
Nachhaltigkeit, Ressourcenschonung, Dienst am Kunden – all das klingt auf dem Papier wunderbar. In der Praxis erleben wir Konsumenten genau das, was angeblich nicht existiert: Obsoleszenz, die von uns mit Sicherheit nicht gewünscht ist.

Foto Darpfeil: Ljupco Smokovski / Shutterstock.com