

Gefahrlos chatten

Sicherheits-Checkliste WhatsApp

In der Voreinstellung hält es WhatsApp in puncto Datenschutz und -sicherheit eher lax. Zum Glück können Sie das Schutzniveau deutlich anheben. Vorsicht ist bei Links in Nachrichten angesagt.

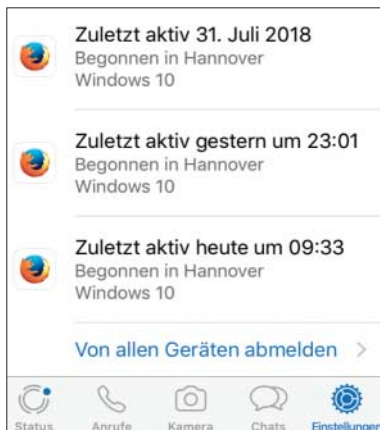
Von Holger Bleich



WhatsApp Web

Viele nutzen WhatsApp nicht nur mobil mit dem Smartphone, sondern auch im Desktop-Browser oder als PC-Anwendung. Dazu müssen Sie zuerst mit der Handy-App einen am Bildschirm angezeigten QR-Code scannen – so verbindet WhatsApp das aktive Handy mit der Webanwendung im Browser. Diese Verknüpfung bleibt bestehen. Wer Zugriff auf den PC hat, könnte folglich dauerhaft jeden Chat mitlesen, den Sie mit dem Smartphone führen.

In der App sollten Sie deshalb im Einstellungsmenü unter „WhatsApp Web“ kontrollieren, welche Geräte derzeit angemeldet sind. Nicht benötigte oder gar unbekannte Geräte können Sie einzeln die Autorisierung entziehen.



Checken Sie in der WhatsApp-App, welche Geräte außerhalb des Smartphones für den Zugriff autorisiert sind.



Backup einschalten

In der Voreinstellung sichert WhatsApp Chat-Verläufe nicht, fragt aber später ab und an nach, ob das so bleiben soll. In den Einstellungen können Sie unter „Chats“ auch jederzeit selbst die Backup-Option aktivieren. Unter Android sichert WhatsApp die Verläufe dann ins Google Drive des Accounts, unter iOS in die iCloud. Ab November rechnet Google das Backup nicht mehr zum Drive-Speicherkontingent hinzu – allerdings ist die Sicherung anders als in der iCloud unverschlüsselt. Ein automatisches Backup sorgt dafür, dass Chats und gespeicherte Dateien beim Geräte-Crash oder -Wechsel nicht verloren gehen.



Öffentliche Infos

Standardmäßig kann jeder, der Ihre Rufnummer kennt, unter anderem Ihr Profilbild abrufen. In den Einstellungen der WhatsApp-App regeln Sie unter Account/Datenschutz, welche Informationen für wen sichtbar sein sollen. Voreingestellt gibt sich WhatsApp sehr offen. Investieren Sie hier einige Minuten in besseren Schutz Ihrer Privatsphäre.



Verifizierung

Sichern Sie Ihr WhatsApp-Konto unbedingt mit der Zwei-Faktor-Authentifizierung ab. Die nicht voreingestellte Option dazu finden Sie unter „Verifizierung in zwei Schritten“ in den Account-Einstellungen. Sie werden aufgefordert, eine sechsstelligen

PIN zu wählen. Notieren Sie diese PIN und nutzen Sie das optionale Eingabefeld für eine Recovery-Mailadresse. Die Eingabe der PIN verlangt WhatsApp künftig nicht vor jedem Start der App, sondern sporadisch, und zwingend beim Rufnummernwechsel – sie schützt also den Account vor feindlicher Übernahme.



Misstrauisch sein

WhatsApp ist aufgrund der hohen Verbreitung ein Liebling von Betrugern verschiedenster Couleur. Oft geht es darum, an Ihre persönlichen Daten zu kommen. Immer wieder etwa versenden Abzocker direkt oder als Kettenbrief Nachrichten, in denen auf angebliche Gutscheine von großen Marken wie Ikea, Milka oder Jägermeister hingewiesen wird. Links in diesen Nachrichten führen dann zu Phishing-Websites, die oft verblüffend gut die echten Markenseiten nachahmen. Seien Sie skeptisch, auch bei Links in Nachrichten befreundeter Kontakte. Fragen Sie lieber noch mal nach, insbesondere, wenn es um einen Short-Link geht, der zu einer unbekannten Quelle weiterleitet.

Nutzen Sie nur die Originalversionen der WhatsApp-Apps. Besondere Vorsicht gilt in Googles Play Store: Immer wieder tauchen hier vermeintlich „verbesserte“ Updates der Original-App auf, die dann beispielsweise „Update WhatsApp Messenger“ heißen, aber bei genauem Hinsehen nicht von der WhatsApp Inc. eingestellt wurden. Mit diesen Apps holen Sie sich potenziell Schadsoftware aufs Smartphone. (hob@ct.de) **ct**