Apps

WhatsApp dienstlich nutzen?

[6.7.2017] Den Nachrichtendienst WhatsApp möchten viele Mitarbeiter der öffentlichen Verwaltung auch für die dienstliche Kommunikation nutzen. Das ist aber unter anderem aus Sicherheits- und Datenschutzgründen bedenklich.

Mobile Applikationen kommen auch im dienstlichen Alltag verstärkt zum Einsatz. Sie erleichtern unter anderem das Finden und Buchen von Hotels oder die Reiseplanung, helfen im Außendienst bei der Adresssuche oder bilden fachliche Anwendungen in einer wachsenden Bandbreite ab. Neben diesen "guten Apps" gibt es auch eindeutig "böse Apps" und dazwischen eine große Grauzone mit vielen Facetten. Eindeutig böse sind Apps, die Daten ausleiten, das Adressbuch übertragen oder das Mikrofon und die Kamera von Smartphones anzapfen, um ihre Nutzer auszuspionieren. Wohl niemand würde eine solche App freiwillig weiter einsetzen, wenn damit kritische Daten in falsche Hände gelangen.

Anfällig für Datenklau

Einige Apps sind nicht von sich aus auf diesen Datenklau aus, sondern lediglich dafür anfällig, dass die von ihnen übertragenen Daten abgefangen werden, wenn sie in die Cloud geladen werden. Leider ist es gerade das Designkonzept von Apps, das sie dafür anfälliger macht als klassische Programme: Denn die Daten werden in der Regel nicht auf dem Endgerät durch die App selbst verarbeitet, sondern im Stil einer klassischen Client-Server-Anwendung von der App zu einem Server in der Cloud zur weiteren Verarbeitung hochgeladen. Anschließend wird das Ergebnis wieder auf das Gerät heruntergeladen und steht dort zur Verfügung ? eine Internet-Verbindung vorausgesetzt. Was für die Anforderungen an die Rechenleistung und damit auch die Akkulaufzeit der mobilen Geräte ein guter Ansatz ist, bedeutet jedoch, dass man die Daten zwingend zur Verarbeitung verschicken und somit sprichwörtlich aus der Hand geben muss. Es ist also an den App-Anbietern, sicherzustellen, dass alle Komponenten in der Kette ? die App selbst, der Datentransfer und der Cloud-Dienst ? vor Angriffen geschützt sind.

Zahl der Spionage-Apps wächst

Mittlerweile gibt es aber auch Erkenntnisse über neue Spionageformen durch Apps. Das geschieht nicht so offensichtlich, wie bei den Apps, die schon bei der Installation die Genehmigung

für alle möglichen Datenquellen auf dem Gerät anfordern, aber dennoch gleichermaßen effektiv. Einige Apps spionieren sogar dann, wenn das Telefon überhaupt keine Datenverbindung hat ? und ihre Zahl wächst besorgniserregend, wie Forscher jüngst herausfanden. Eine Studie der Technischen Universität Braunschweig fand sogar im offiziellen Google Play Store 234 Apps, die zum Beispiel über Ultraschall-Tracking-Technologien die Aktivitäten der Nutzer offline verfolgen. Im Dezember 2015 war die Zahl solch perfider Spionage-Apps mit insgesamt 45 noch deutlich geringer.

Gut oder böse?

Was ist nun aber mit der Grauzone? Mit den Apps, die für nützlich und wichtig, ja sogar für absolut essenziell erachtet werden? Zu den mit Abstand am meisten diskutierten Anwendungen zählt zweifelsohne WhatsApp. Allein schon aufgrund ihrer Relevanz am Markt mit weltweit mehr als einer Milliarde aktiver Nutzer muss man die Applikation auch im dienstlichen Alltag einer Behörde betrachten. WhatsApp tat sich lange schwer damit, seinen Nutzern selbst grundlegende Sicherheit, wie eine funktionierende Verschlüsselung der übertragenen Daten, zu bieten. Erst nach langem Hin und Her wurde dies geändert und eine Ende-zu-Ende-Verschlüsselung eingeführt, die zumindest nach heutigem Verständnis als ausreichend sicher gelten darf. Die Verschlüsselung der Datensicherungen in der iCloud wurde sogar noch später eingeführt. Zur Betrachtung von WhatsApp und letztlich seiner Einstufung zwischen "gut" und "böse" ist es aber zu kurz gegriffen, nur die technische Implementierung von Sicherheit zu betrachten.

Schnell und einfach kommunizieren

Als IT-Dienstleister der Stadt Dortmund wird das Dortmunder Systemhaus häufig gebeten, WhatsApp für die dienstliche Nutzung bereitzustellen. Die Einsatzszenarien sind dabei breit gefächert. In der Regel geht es um eine schnelle Erreichbarkeit im Notfall und die Vereinfachung von Kommunikation, zum Beispiel in der Jugendsozialarbeit. In den meisten Fällen ist den Nutzern jedoch nicht bewusst, dass WhatsApp seinen Dienst ausschließlich für die rein private Nutzung bereitstellt. Das ist in den Nutzungsbedingungen klar geregelt.
Auch die Übermittlung von Daten an den WhatsApp-Mutterkonzern Facebook stößt bei Datenschützern auf wenig positives Echo. Das Unternehmen war im Jahr 2014 von Facebook übernommen worden und hatte im August 2016 bekannt gegeben, künftig zwar keine Inhalte der Kommunikation, sehr wohl aber Nutzungs- und Metadaten an seinen Mutterkonzern übermitteln zu wollen. Das veranlasste den Hamburger Datenschutzbeauftragten Johannes

Caspar im September 2016 dazu, Facebook genau dies für die etwa 35 Millionen deutschen Nutzer per Bescheid zu untersagen und zudem die sofortige Vollstreckung gemäß § 80 Abs. 2 Nr. 4 Verwaltungsgerichtsordnung (VwGO) anzuordnen. Die sich anschließende gerichtliche Auseinandersetzung am Verwaltungsgericht Hamburg (Az. 13 E 5912/16) hat dabei auch die Frage behandelt, ob für WhatsApp vor dem Hintergrund des Firmensitzes in Irland das deutsche Datenschutzrecht überhaupt anwendbar ist.

Im dunklen Bereich der Grauzone

Obwohl das Gericht die Rechtslage für noch nicht abschließend geklärt hält, entschied es, dass das Interesse der deutschen Nutzer am Übermittlungsverbot überwiege. Eine maßgebliche Rolle spielte dabei die Unwirksamkeit des Einwilligungsverfahrens. So sei etwa die Zustimmung zur Datenverarbeitung gemäß § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) durch die Gestaltung des Willkommensbildschirms beim ersten Start der Anwendung nicht erkennbar. Das Urteil vom 27. April 2017 bestätigt insofern das Verbot der Datenverarbeitung und -erhebung auf Vorrat sowie den Vorrang der Interessen aus dem Grundrecht auf informationelle Selbstbestimmung.
Bis die Rechtslage abschließend geklärt ist und WhatsApp auch eine nicht-private Nutzung zulässt, ist seine dienstliche Verwendung im tiefdunklen Bereich der Grauzone anzusiedeln. Was bleibt, ist der enorme Erwartungsdruck der Anwender und ein Mangel an alternativen Anwendungen mit einem akzeptablen Verbreitungsgrad.

Stefan Klebs ist Leiter des Teams Infrastrukturdienste beim Dortmunder Systemhaus.

www.dortmund.de
Dieser Beitrag ist in der Juli-Ausgabe von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren. (Deep Link)

Stichwörter: IT-Sicherheit, Apps, Dortmund

Quelle: www.kommune21.de