Datenschleuder

Massive Datenschutzmängel in der Gesundheits-App Ada

Gesundheits-Apps wie die der Ada Health GmbH verarbeiten besonders sensible Daten und betonen gerne, dass ihnen die Privatsphäre der Nutzer wichtig sei. Doch eine Analyse des Datenverkehrs belegte, dass die Ada-App Gesundheitsdaten an Dritte weitergab.

Von Sylvester Tremmel, Hartmut Gieselmann und Ronald Eikenberg

Der Schutz Ihrer Daten, Privatsphäre und personenbezogenen Daten ist für (uns) sehr wichtig.“ Solche Sätze liest man mittlerweile in so vielen Datenschutzerklärungen, dass der Eindruck entsteht, sämtliche Unternehmen wären zu Datenschutzvorreitern geworden. Aktuelle Analysen wecken jedoch arge Zweifel an der Ernsthaftigkeit dieser Formulierungen.

Der obige Satz stammt aus der Datenschutzerklärung zur App „Ada“, entwickelt von der deutschen Ada Health GmbH mit Hauptsitz in Berlin. Ada ist eine Art Chat-Programm, das den Nutzer nach Symptomen befragt, auf mögliche Erkrankungen hinweist und gegebenenfalls rät, einen Arzt aufzusuchen. Bekannt wurde die kostenlose App unter anderem, weil die Techniker Krankenkasse mit dem Unternehmen kooperiert, sodass die App Versicherten der TK passende Angebote unterbreiten kann. In den App-Stores von Google und Apple rangiert sie unter den populärsten Gesundheits-Apps.

Über bedenkliche Formulierungen in der Datenschutzerklärung von Ada Health haben wir bereits berichtet [1]. Inzwischen sah sich der Experte für IT-Sicherheit Mike Kuketz das tatsächliche Verhalten von Ada unter Android an – insbesondere welche Daten Ada wann wohin überträgt – und beschrieb gravierende Probleme.

Ada nutzt Tracking- und Analyse-Dienstleister wie Amplitude, Adjust und Facebook und weist darauf in der Datenschutzerklärung hin. Allerdings wurden laut Kuketz sowohl an Facebook als auch an Amplitude Daten versendet, bevor die App dem Nutzer AGB und Datenschutzerklärung präsentierte und ihn um die Akzeptanz derselben bat. Selbst wenn der Nutzer also die Zustimmung verweigerte und die App beendete, waren nach Kuketz’ Erkenntnissen bereits Daten an Facebook und Amplitude abgeflossen.

Juristisch ist eine solche Übertragung äußerst zweifelhaft: Die DSGVO schreibt nämlich vor, dass bei der Erhebung personenbezogener Daten die betroffene Person „zum Zeitpunkt der Erhebung dieser Daten“ informiert werden muss. Die App übertrug jedoch schon vorher – Ada schien hier zumindest sehr frei zu interpretieren, was ein Zeitpunkt ist.

Schwammige Erklärungen

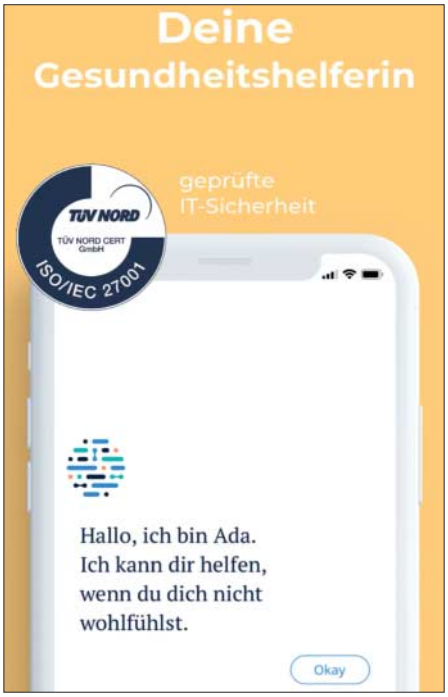
Zu den übertragenen Daten gehörten nicht nur technische Informationen zum Smartphone und Betriebssystem, sondern nach dem Einloggen auch die vom Nutzer eingegebenen Symptome: „Zunächst wird gefragt, ob es um mich geht oder um jemand anderen. Danach soll ich eingeben was mich ‚am meisten beschäftigt‘. Ich gebe zu Testzwecken mal Inkontinenz ein. Das wird dann gleich auch an Ada übermittelt [...] Aber nicht nur an Ada, sondern gemeinsam mit anderen Informationen auch an den Amplitude-Tracker“, schrieb Kuketz in seinem Blog.

Auf Nachfrage von c’t erklärte die Ada Health GmbH in Reaktion auf die von Kuketz nachgewiesene Übertragung der Krankheitssymptome an Amplitude: „Dritte haben keinen Zugriff auf persönliche Gesundheitsinformationen der User. Facebook, Adjust oder Amplitude erfahren folglich nicht, ob ein User beispielsweise angibt, Bluthochdruck zu haben oder wo er versichert ist.“

Daraufhin stellten wir unsere eigenen Analysen an, mit der zu dem Zeitpunkt aktuellen Version 2.49.0 der App. Dabei konnten wir nicht nur die Funde von Kuketz bestätigen, sondern darüber hinaus den Datenverkehr zu Facebook einsehen: Die Ada-App übertrug unter anderem den Namen der Krankenversicherung des Nutzers. Das erstaunt, steht doch in der Datenschutzerklärung der Ada Health GmbH, dass „keine Profilinformationen der Ada App und auch keine medizinischen Daten an Facebook übermittelt“ würden.

Mit unseren Ergebnissen konfrontiert, erklärte die Firma nun, dass sie einen „eigenen, geschützten Bereich innerhalb von Amplitude“ habe, „auf welchen Amplitude keinen Zugriff hat.“ Das sei „durch entsprechende Verträge abgesichert“.

Die in den USA ansässige Analysefirma Amplitude räumt sich in ihren AGBs jedoch durchaus vertragliche Zugriffsrechte ein, um ihren Service überhaupt



Ada bewirbt seine Gesundheits-App mit einem Prüfsiegel des TÜV. Der hatte offenbar nichts gegen die Datenübermittlungen einzuwenden.

anbieten zu können. Adas Verträge mit Amplitude mögen von den Standard-AGBs abweichen, aber prinzipiell braucht Amplitude Zugriff auf die Daten, schon um sie entgegennehmen zu können. Darüber hinaus dürfen US-Behörden im Rahmen des Cloud-Acts jederzeit auf die Daten zugreifen, ohne dass der Nutzer davon etwas erfährt.

Pseudonyme Identifikation

Auf Nachfrage, warum die Symptome und Versicherungsdaten überhaupt an Fremdfirmen übertragen wurden, gab uns Ada Health keine Auskunft. Mehr noch, die Firma stritt die Brisanz der Datenübertragung ab: „Dies ist ein übliches Vorgehen. Die Behauptung, dass Amplitude Personen identifizieren kann, ist folglich falsch“, teilte uns ein Sprecher mit.

Was Amplitude mit den Daten machen kann oder nicht, hängt jedoch davon ab welche anderen Quellen Daten an die Firma übertragen. Prinzipiell lassen sich umfangreiche Profile anlegen, wie eine vor Kurzem im British Medical Journal veröffentlichte Studie zeigt. Die Forscher analysierten den Datenverkehr von 24 Gesundheits-Apps, einschließlich Ada. Unter den getesteten Apps war Ada diejenige, die Daten an die größte Zahl von Drittfirmen übermittelte. Wenn die Daten erst einmal dort gelandet sind, gibt es kaum noch Möglichkeiten, die Weitergabe an weitere Subunternehmer (sogenannte Viertfirmen) zu kontrollieren. Die australischen Forscher konnten im gesamten Testfeld über 200 solcher Viertfirmen ermitteln, die potenziellen Zugriff auf Daten von Gesundheits-Apps haben.

All diesen Firmen steht prinzipiell die Möglichkeit offen, Daten aus verschiedenen Quellen zu umfangreichen Dossiers über die Nutzer zusammenzuführen. Ausreichend anonymisiert sind die Daten nämlich in der Regel nicht. Auch die Ada-App übermittelte nicht etwa nur die Symptombeschreibung an Amplitude, sondern reicherte sie zusätzlich mit diversen Metadaten an, wie dem Geschlecht des Nutzers und der Android Advertising-ID.

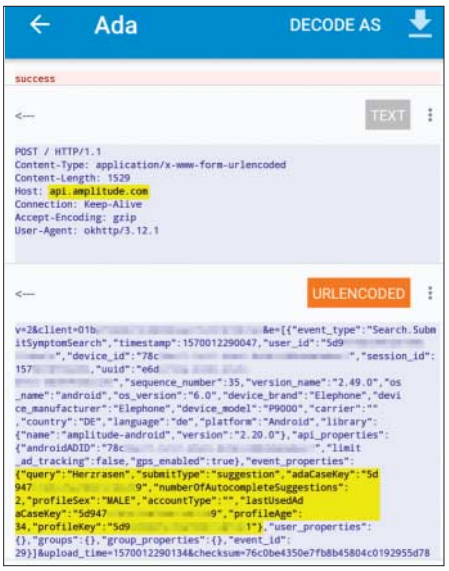
Eine solche Werbe-ID lässt sich zwar vom Nutzer wechseln. Da dies jedoch nur wenige regelmäßig tun, lassen sich der ID zugeordnete Daten oft zu detaillierten Profilen ergänzen: Die australischen Forscher konnten das ungefähre Alter, Geschlecht, den Wohnort, die Hobbys und Interessen, Krankheitssymptome und Medikamentation ihres Testprofils zusammenführen. Schon mit nur einem Bruchteil dieser Parameter sind Nutzer häufig eindeutig zu identifizieren.

Bei einer genaueren Analyse der Datenschutzbestimmungen von Ada fielen uns zudem Unterschiede zwischen der deutschen und der englischen Version auf. Letztere sei laut Ada die offizielle Fassung und bei Diskrepanzen maßgebend. Da wurde aus „... um unbefugten Zugriff zu verhindern“ der bloße Versuch mit „... to try to prevent unauthorised access.“ Ein deutscher Absatz zur Nutzung von Name, Geburtsdatum, Facebook-Benutzername und Passwort fehlte in der englischen Fassung komplett und gleich am Anfang redete die englische Variante von „your rights“, also Rechten des Nutzers (an seinen Daten), während die deutsche von „unseren Rechten“, also Rechten von Ada sprach. Da fielen diverse kleinere Abweichungen und technischen Ungenauigkeiten (etwa „SSL“ und nicht „TLS“) kaum noch ins Gewicht. Solche Unterschiede, die deutschsprachige Leser dann selbst mit Hilfe der englischen Fassung entdecken sollen, sind kaum DSGVO-konform. Die erfordert nämlich, dass Regelungen „verständlich und in klarer und einfacher Sprache abgefasst sind“.

Nachbesserungen

Von uns zu dem Ergebnis der Analyse befragt betonte die Pressereferentin der Techniker Krankenkasse, dass „zu keiner Zeit Daten zwischen Ada und der TK ausgetauscht“ würden. Die zuständige Datenschutzbeauftragte des Landes Berlin teilte uns auf Nachfrage mit, dass die Ada Health GmbH der Behörde zwar bekannt sei, die App aufgrund von Personal- und Ressourcenmangel bislang jedoch nicht überprüft werden konnte.

Allerdings verstieß Ada wohl auch gegen die Nutzungsbedingungen von Google, die erfordern, dass die Werbe-ID „nur mit ausdrücklicher Zustimmung des Nutzers mit personenbezogenen Daten [...] verknüpft werden“ darf. Google äußerte sich auf die konkrete Anfrage von c’t nur allgemein: „Wenn Apps gegen diese Richtlinien verstoßen, handeln wir entsprechend.“ Kurz vor Redaktionsschluss überschlugen sich daraufhin die Ereignisse – offenbar durch die Recherche von c’t: Zuerst verschwand die Ada-App aus dem Play-Store, am 4. Oktober tauchte sie dann wieder auf – in der neuen Version 2.49.1. In einem kurzen Check konnten wir keine Datenübertragungen an Amplitude mehr feststellen.



Ada 2.49.0 übermittelte Symptombeschreibungen (hier „Herzrasen“) an Amplitude. Die Übertragung protokollierten wir mit Packet Capture.

Das Verhalten und die Reaktionen von Ada zeigen, dass in puncto Datenschutz bei Gesundheits-Apps offenbar großer Nachholbedarf besteht. Das sieht auch die große Mehrheit der deutschen Bevölkerung so, wie eine Studie des Büros für Technikfolgenabschätzung beim Deutschen Bundestag ergab: Mehr als 80 Prozent der Deutschen wünschen sich, dass für Gesundheits-Apps „verbindliche Standards für Qualität, Datenschutz und Datensicherheit etabliert werden“, dass „die Einhaltung datenschutzrechtlicher Anforderungen durch App-Hersteller und App-Store-Betreiber stärker kontrolliert werden sollte“ und dass „App-Hersteller und App-Store-Betreiber Selbstverpflichtungen eingehen sollten, um die Privatsphäre von App-Nutzern besser zu schützen.“

Vor diesem Hintergrund sollte nicht zuletzt Gesundheitsminister Jens Spahn den Entwurf des Digitale-Versorgung-Gesetz (DVG) nachbessern, das künftig eine Kostenerstattung der Krankenkassen von Gesundheits-Apps auf Rezept vorsieht. Der Gesetzentwurf wurde nach einer ersten Lesung Ende September zur Nachverhandlung in die Ausschüsse gegeben.

(syt@ct.de) c't

Literatur

[1] Hartmut Gieselmann, Risiken und Nebenwirkungen, c’t 17/2019, S. 60

Studien und Analysen: ***ct.de/ydd8***