PRESSEMITTEILUNG

Pressekontakt

Sebastian Wolters | CEO

wolters@appvisory.com
Telefon +49 (0)511 35 39 94-20
Fax +49 (0)511 35 39 94-12

Hannover, 11. April 2020

mediaTest digital prüft Sicherheit der „Corona-Datenspende“-App

- **Android und iOS-Version der aktuell meistgeladenen App weisen keine Sicherheitsmängel auf (CVSS Score 2.0*) und halten ihr Versprechen, die Daten in Deutschland zu belassen**
- **Datenschutzstrategie nicht optimal (Pseudonymisierung statt Anonymisierung, Closed Source Strategie)**
- **Ausführender App-Entwickler ist ein Berliner Start-Up, das mit Medizindaten handelt**

Ganz Deutschland wartet gespannt auf die von der Regierung und dem Rober-Koch-Institut (RKI) angekündigte Corona-App. In der Öffentlichkeit wird bereits heiß über Sicherheit und Datenschutz der Anwendung diskutiert. Im Vorfeld der Veröffentlichung hat das RKI nun eine App zur Corona-Datenspende in Verbindung mit Fitness-Trackern auf den Markt gebracht, die in den App-Stores sofort auf Platz 1 der meistgeladenen Apps geschossen ist. Deutschlands führender App-Security Anbieter mediaTest digital hat sich die Android- und iOS-Versionen der App mit Hilfe seiner beiden Testverfahren „Appscan“ (vollautomatisierte statische Analyse) und „PrePentest“ (manuelle, dynamische Prüfung durch Security-Analysten) angeschaut und kann erfreulicherweise verkünden, dass die App vorerst bedenkenlos genutzt werden kann. Die Verschlüsselungsmechanismen sind sauber integriert und es werden keine sensiblen Daten unverschlüsselt und außerhalb von Deutschland übertragen. Der "Man-in-the-Middle" Angriff war dem Testlabor nur mit erheblichem Aufwand möglich, da seitens der Programmierer mit Certificate Pinning und TLS1.3-Verschlüsselung für alle wichtigen Verbindungen der richtige Ansatz gewählt wurde.

Zum Schutz der Daten wird beim ersten Start der App ein Pseudonym bestehend aus User-ID und Postleitzahl generiert, das für den Nutzer sichtbar ist. Wie aus diversen anderen Fällen bekannt ist, können solche Pseudonyme recht einfach wieder realen Personen zugeordnet werden. Daher wäre an dieser Stelle eine Anonymisierung aus Datenschutzgesichtspunkten wünschenswert. Darüber hinaus betont mediaTest digital, dass eine App, die mit solch sensiblen und vertrauenswürdigen Daten hantiert, Open Source entwickelt werden sollte, wie es diverse Apps bereits tun (z.B. Firefox oder Signal). Die Closed Source Entwicklung führt dazu, dass mit jedem Update der App ein erneuter Sicherheitstest stattfinden muss, um das Vertrauen aufrecht zu erhalten und Datenpannen auszuschließen. Hierzu empfiehlt mediaTest digital, die kürzlich vom Chaos Computer Club (CCC) in Bezug auf die Corona-Pandemie bekanntgegeben 10 Prüfsteine zur Beurteilung von „Contact Tracing“-Apps (https://www.ccc.de/de/updates/2020/contact-tracing-requirements)

einzuhalten, was bei einer Closed Source App wie der „Corona-Datenspende“ nicht möglich ist.

In der aktuellen Version werden die Gesundheitsdaten aus den Fitness-Trackern nicht in der App verarbeitet. Dies könnte sich jedoch in zukünftigen Versionen ggfs. ohne Wissen der Nutzer ändern, was ebenfalls das notwendige erneute Testen der App bei jedem Update unterstreicht. „Da die App nicht Open-Source ist und jedes Update das Verhalten der Applikation vollumfänglich ändern kann, ist dieses Ergebnis nur als Momentaufnahme zu verstehen und kann nicht als generelle und immer gültige Aussage zum Sicherheitsniveau der App verstanden werden. Es ist denkbar, dass durch zukünftige Änderungen der App die ohnehin diskussionswürdige Pseudonymisierung aufgeweicht wird und zusätzliche eindeutige Geräte-Identifier zur genaueren Personenbestimmung ohne Wissen der Bürger mit übertragen werden.“ betont Wulf Bolte, CTO bei mediaTest digital.

Dem Nutzer sollte darüber hinaus zumindest bewusst sein, dass die für die App verantwortliche Entwicklerfirma ein Berliner Startup namens "mHealth Pioneers GmbH" ist, das sich mit seinem Produkt „Thrive“ das Verwerten von Medizin- und Gesundheitsdaten auf die Fahne geschrieben hat. „Hieraus wird deutlich, dass mit den generierten Daten durchaus auf anderen Wegen Geld verdient werden kann. Es ist aus unserer Sicht zumindest fragwürdig, einen Datenverwerter mit einer hochsensiblen Datenerfassungs-App dieser Art zu beauftragen. Da es sich um eine Datenspende handelt, ist im Falle des Verkaufs der Firma unklar, was mit den erhobenen Daten passiert. Sinnvoller und transparenter für den Bürger wäre eine echte Anonymisierung der erfassten Daten und die Veröffentlichung mittels OpenData (https://www.bpb.de/gesellschaft/digitales/opendata/)“ gibt Bolte zu Bedenken. Des Weiteren ist anzumerken, dass die Analyse von mediaTest digital sich auf das Datensendungsverhalten der App beschränkt, so dass keine Rückschlüsse auf die Sicherheit und Lokalisation der involvierten Server seitens der Fitness-Tracker wie Fitbit & Co gezogen werden können.

**Der CVSS-Score gibt in einer Skala von 0 bis 10 aufsteigend Auskunft über die Gefährlichkeit einer App (und anderer IT-Systeme) hinsichtlich Datenschutz und Datensicherheit. https://www.first.org/cvss/*

Über mediaTest digital

mediaTest digital ist mit seiner Software APPVISORY® und seinem Gütesiegel TRUSTED APP Europas führender App-Security-Anbieter. Die Mobile Application Management Lösung stellt den Schutz sensibler Unternehmensdaten bei der Nutzung mobiler Endgeräte sicher. Mithilfe von APPVISORY setzen Unternehmen ihre individuellen IT-Sicherheitsrichtlinien sowie Vorgaben laut Bundesdatenschutzgesetz (BDSG) und der neuen EU-Datenschutzgrundverordnung (DSGVO) auf allen Mitarbeitergeräten durch. Gleichzeitig trägt APPVISORY mit seinem App-Client zur Aufklärung und Sensibilisierung der Anwender bei und fördert die Nutzung von Apps und damit die Digitalisierung und Mobilisierung von Geschäftsprozessen. mediaTest digital sichert weltweit betrieblich genutzte Smartphones und Tablets von mehreren Hundert Kunden in der Größe von drei bis 50.000 Endgeräten ab. Diverse Dax30-Unternehmen sowie zahlreiche mittelständische und kleine Unternehmen aus Wirtschaftszweigen wie Banken, Automotive, Energieversorgung oder Behörden zählen heute zu den zufriedenen Kunden. Das in Deutschland ansässige Unternehmen nutzt ausschließlich deutsche Server für das Hosting und die Entwicklung seiner Lösungen. Mehr Informationen zu APPVISORY finden Sie auf www.appvisory.com.