Published on *Management-Krankenhaus.de* (https://www.management-krankenhaus.de)

09.10.2018

Völlig unsichere Gesundheits-Apps?

Der Präsidiumsarbeitskreis „Datenschutz und IT-Sicherheit“ der Gesellschaft für Informatik e.V. (GI) begrüßt im Rahmen der Digitalisierung ausdrücklich das zunehmende Angebot an Gesundheits-Apps für die über 80 Millionen Versicherten – warnt aber gleichzeitig vor allzu unbegründetem Vertrauen in die bisherigen Entwicklungen und die nicht überprüften Versprechungen hinsichtlich Datenschutz und IT-Sicherheit.

Allein mit der neuen gemeinsamen Gesundheits-App „Vivy“ von 13 gesetzlichen und zwei privaten Krankenversicherungen sollen ca. 13,5 Millionen Kunden zukünftig verstärkt Gesundheitsservices übers Handy abrufen können. Prof. Dr. Hartmut Pohl, Sprecher des GI-Präsidiumsarbeitskreises „Datenschutz und IT-Sicherheit“ weist auf die Risiken der neuen Apps hin: „Die angebotenen Funktionen mögen tatsächlich funktionieren. Die entscheidendere Frage bei dem Abruf von Gesundheitsdaten (elektronische Patientenakte) ist aber, wer liest Befunde, Blutwerte, Medikationspläne, Impfpässe und Röntgenaufnahmennoch mit und noch schlimmer, an wen werden Daten versandt und wer kann die Gesundheitsdaten verändern?“

Eine App steht nämlich nicht allein. Vielmehr hängt das Sicherheitsniveau von den folgenden Aspekten und Komponenten ab:

- Gesundheits-Apps laufen auf Hardware wie Handys und Tablets und Betriebssystemen, die erfahrungsgemäß von Angreifern ausnutzbare Sicherheitslücken enthalten. Ein Handy kann von Angreifern auch dann erfolgreich genutzt werden, wenn der Versicherte den Ausschalter betätigt hat: Der Versicherte erkennt dabei nicht, dass sein Handy über das Mobilfunknetz wieder eingeschaltet und missbraucht wird.

- Angreifer brauchen weder Nachrichtendienste noch organisierte Kriminelle zu sein – es können auch die Nachbarskinder sein, die einen Angriff im Internet ‚gefunden' haben und an Versicherten ausprobieren. Angriffe gibt's übrigens fertig und entgeltfrei u.a. bei Metasploit. Man muss die Angriffe noch nicht einmal verstehen, um andere Nutzer erfolgreich zu hacken.

- Alle mit der App kommunizierenden Servervon Krankenhäusern, Arztpraxen, Laboren und andere zur Verwaltung der medizinischen Daten (Krankenkassen, Versicherungen) verwendete Rechner, Service Provider, Clouds stellen ein Risiko für die Vertraulichkeit und Integrität der gespeicherten und bearbeiteten Gesundheitsdaten dar.

Dazu gehören neben den explizit für die Verarbeitung dieser Daten eingesetzten Server auch Zwischenknoten. Weiterhin bietet die von der App zum Schutz der Übermittlung eingesetzte TLS-Verschlüsselung keinen Schutz gegen einen Missbrauch der Daten auf den Servern, da sie nur eine Leitungsverschlüsselung unterstützt, so dass die Daten auf diesen Servern im Klartext vorliegen.

- Gesundheits-Apps können durch andere Apps manipuliert werden! Und über diese Manipulationen ist auch eine Infektion anderer Apps möglich, die auf einem von Schadsoftware befallenen Endgeräte des Nutzers laufen (Viren, Würmer, Trojanische Pferde, …). Das insgesamt erreichbare Sicherheitsniveau dürfte sehr gering sein; selbst die zur Verschlüsselung eingesetzten kryptographischen Schlüssel sind dann nicht sicher!

Zusätzlich gibt es weitere Sicherheitslücken:

- Einige Gesundheits-Apps verbinden sich direkt nach dem Start, vor der allerersten Benutzereingabe (Versicherten-Nr., Passwort) mit mehreren Tracking-Diensten auch außerhalb der EU, und übermitteln diverse Daten an diese Dienste, zu denen u.a. auch die IP-Adresse des Versicherten gehört. Diese Daten erlauben in

der Regel eine Re-Identifikation des Gerätes, so dass sie mit anderen personenbezogenen Daten verknüpft werden können, die andere Apps auf demselben Gerät an den betreffenden Tracking-Dienst übermitteln. Welche Daten übermittelt werden, ist dabei weder ausreichend dokumentiert noch wegen der teilweise verwendeten Verschlüsselung vollständig überprüfbar.

- Auch die Datenschutzerklärung hilft an dieser Stelle nicht weiter, wenn ihr erst zugestimmt werden kann, nachdem schon längst Daten übermittelt wurden (etwa zum Tracking). Davon abgesehen, wird in der Datenschutzerklärung meist auch nicht in vollem Umfang beschrieben, an wen welche Daten übermittelt werden. Es ist deshalb auch nicht ersichtlich, welche Informationen aus den übermittelten Daten und den damit bei den Tracking-Diensten aus anderer Quelle bezogenen Daten abgeleitet werden.

- Damit ist es über Profilbildung in vielen Fällen möglich, das Gerät und oft auch den Nutzer, den Versicherten zu ermitteln und dessen Identität mit den übertragenen Daten dieser App und auch anderer Apps, zu verknüpfen. So lassen sich beispielsweise Rückschlüsse auf das Surf-Verhalten des Versicherten, auf Einkäufe und auch eine Vielzahl anderer Aktivitäten ziehen.

- Die Übertragung dieser Daten ohne vorherige Einwilligung des Versicherten stellt einen Verstoß gegen die EU-DSGVO dar (EU-DSGVO, Art. 4 Abs. 1): Sie dürfen erst nach expliziter Freigabe durch den Nutzer übermittelt werden.

- Wenn so Dritten Zugriff auf Gesundheitsdaten ermöglicht wird, liegen sogar strafbare Handlungen gemäß § 203 ff. StGB seitens der Verantwortlichen zu Lasten der Versicherten vor.

- Durch die Gesundheits-Apps entstehen insgesamt für die höchst schützenswerten medizinischen Daten der Versicherten unkalkulierbare Risiken weil Handys und Tablets grundsätzlich nur ein geringes Sicherheitsniveau erlauben.

Stand der Technik zur Sicherheitsprüfung generell von Software und auch mobiler Apps ist der langjährige internationale Standard ISO/IEC 27034, der konkrete Vorschläge für die Entwicklung sichererer Software und Apps macht. Mindestens diese Norm muss zugrunde gelegt werden, und die zugehörigen Prüfberichte und Zertifikate müssen veröffentlicht werden; dazu gehört die Angabe des zertifizierten Bereichs (GUI – Bedienoberfläche oder Security etc).

Kontaktieren

Gesellschaft für Informatik e.V.
Anna-Louisa-Karsch-Str.2

10178 Berlin