Datensicherheit von Medical Apps – eine Stichprobe

Urs-Vito Albrecht, Oliver Pramann, Christoph Noll, Tobias Jungnickel, Ute von Jan

EXECUTIVE SUMMARY

Die Sammlung von persönlichen Informationen durch Serviceanbieter ist eine wertvolle Basis zur Erstellung von Nutzerprofilen für zielgruppenspezifische Werbung. Mobile Geräte vereinfachen diesen Sammelprozess. Unabhängig von der Anwendung, ist dieses Verhalten von den Nutzern meist unerwünscht. Mobile medizinische Anwendungen zielen oft auf spezifische Gesundheitsfragen. Damit entstehen sehr sensible Daten. In diesem Zusammenhang ist es von Bedeutung, ob eine solche Anwendung vertrauenswürdig ist oder nicht.

Im vorliegenden Bericht wird anhand einer kleinen Stichprobe von acht zufällig ausgewählten medizinischen Apps der Umgang mit spezifischen Aspekten des Datenschutzes und der Privatsphäre untersucht. Von den getesteten Anwendungen waren nur drei in Bezug auf eine mögliche Verletzung der Privatsphäre oder Sicherheit durch Übertragung von Daten unkritisch zu werten, da hier keine Datenübertragung stattfindet. Drei Apps sind im Handling der anvertrauten Daten kritisch zu bewerten, da sie die Daten unverschlüsselt übertragen. Zwei dieser Apps übermittelten identifizierende Daten ohne Wissen der Nutzer.

Auch ohne eine Analyse des Netzwerkverkehrs können Nutzer anhand von wenigen Faktoren eine eigene Einschätzung über das Datenschutzniveau treffen. Hierzu können sie Kriterien wie potentielle bzw. tatsächlich stattfindende Datenerhebung und -übertragung heranziehen und sollten auch die Deckungsgleichheit mit der betreffenden Datenschutzerklärung abgleichen.

Inhaltsverzeichnis

RISIKEN BEI DER DATENVERARBEITUNG DURCH MEDICAL APPS

Mobile Technologien und die darauf eingesetzten Applikationen (Apps) sind für viele Nutzer nicht mehr aus dem Alltag wegzudenken. Obwohl diese Geräte primär für den allgemeinen privaten und geschäftlichen Einsatz konzipiert wurden, werden sie – sowohl auf ärztlicher Seite als auch bei Patienten – zunehmend auch im medizinischen Bereich eingesetzt. Zu nennen sind hier u.a. die Nutzung als Informationsplattform zum Nachschlagen von Medikamenten und Behandlungen, zur Literaturrecherche oder – im professionellen Umfeld – zum Management der Patientendaten.

Verschiedene Faktoren tragen zur Sicherheit mobil eingesetzter Applikationen bei. Der Anwender hat hier teils nur eingeschränkte Eingriffsmöglichkeiten, sollte sich aber dennoch aller beitragenden Faktoren bewusst sein. Netzwerk, Hardware, Betriebssystem und die eingesetzten Apps selbst können Sicherheitslücken aufweisen, die einen Datenmissbrauch ermöglichen (Abb. 1).

Im vorliegenden Bericht wurde der App- und der Netzwerkaspekt dieser Sicherheitskette hinsichtlich der Frage untersucht, ob sensible Daten ohne entsprechende Information des Nutzers versendet werden, ob gängige Regeln im Datenhandling berücksichtigt wurden und ob der Datentransfer entsprechend gesichert erfolgt.

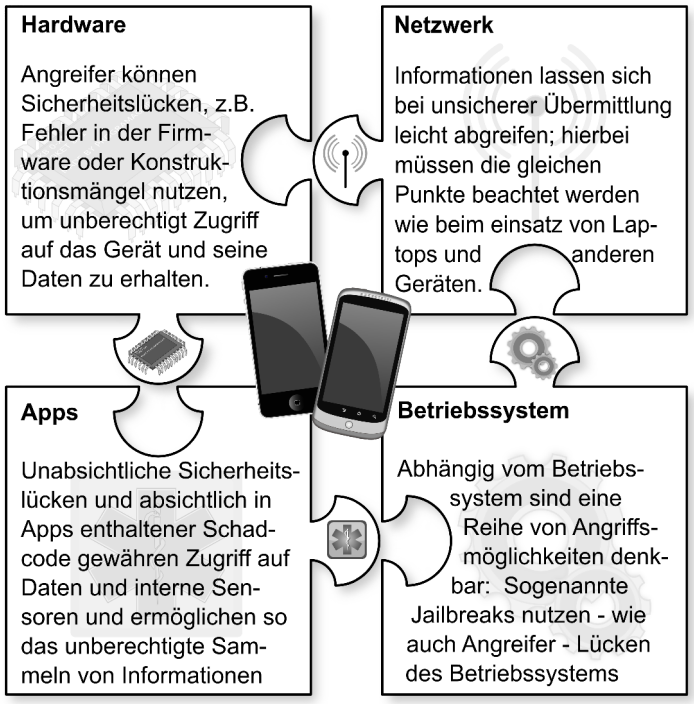

Abb. 1. Faktoren, die die Sicherheit der Datenverarbeitung mittels mobiler Apps beeinflussen

ANALYSE VON ACHT ZUFÄLLIGEN MEDICAL APPS

Die Ergebnisse basieren auf einer zufälligen Auswahl von Applikationen aus der deutschsprachigen Kategorie “Medizin” des AppStore® von Apple® und – soweit vorhanden – den jeweiligen Android-basierten Pendants. Drei Reviewer wählten die ersten acht Applikationen aus, die aufgrund ihrer Beschreibung zumindest ansatzweise einen medizinischen Zweck erfüllen und bei denen eine Datenerfassung, Speicherung sowie Transfer sensibler Daten zu vermuten ist. Nutzungsbedingungen und Datenschutzerklärungen der jeweiligen Apps wurden bei der Analyse berücksichtigt.

Die Applikationen wurden nach Zurücksetzten auf die Werkseinstellungen der jeweiligen Geräte einzeln auf die Smartphones installiert und einer Netzwerkverkehranalyse unterzogen. Genutzt wurden ein iPhone 3GS (iOS 4.3.3), ein iPod Touch (iOS 5.1.1), ein HTC Desire HD (Android 2.3.3) und ein Sony Ericsson Xperia mini pro (Android 2.3.4).

Zur Analyse des Netzwerkverkehrs wurde ein privates Funknetzwerk über einen PC (Linux, Ubuntu 12.04) eingerichtet. Der Netzwerkverkehr wurde mittels der Anwendung Wireshark protokolliert und bezüglich der folgenden Fragen analysiert:

- Werden (persönliche) Informationen abgefragt, die für den angegebenen Zweck der Applikation unnötig sind?
- Gibt es potentiell einen Datentransfer ohne Wissen des Nutzers?
- Entspricht das Datenhandling dem Stand der Technik und werden entsprechende Sicherheitsstandards beachtet?
- Wie gut spiegeln die Datenschutzerklärung und Nutzungsbedingungen das Datenhandling wieder?

Die Apps kommunizierten im Wesentlichen über HTTP bzw. HTTPS mit den jeweiligen Servern; eine programmbezogene Kommunikation unter Nutzung anderer Protokolle wurde nicht festgestellt. Es wurden keine Entschlüsselungsversuche bei verschlüsselter Übertragung unternommen.

DATENSICHERHEIT IN DER STICHPROBE

Betrachtet man die ausgewählten Apps hinsichtlich der oben genannten Fragestellungen, so ergibt sich ein heterogenes Bild. Von acht ausgewählten Apps decken lediglich drei alle erwähnten Aspekte zufriedenstellend ab. . Bei zwei Anwendungen sind selbst vorhandene Datenschutzerklärungen nicht vollständig bzw. nicht gut an den Anwendungsfall angepasst oder räumen den Anbietern unnötige Rechte ein. Drei Applikationen erfassen und übertragen ohne Zustimmung oder Kenntnis der Anwender Daten wie Geräte-IDs. Damit wird ein Tracking (Aufzeichnung und Auswertung des Nutzungsverhaltens) der Anwender, eventuell auch im Kontext anderweitig gewonnener Daten, z.B. durch eine Verknüpfung mit Daten aus anderen Informationsquellen, ermöglicht. In drei Fällen fehlen auch Verschlüsselungsmechanismen beim Datentransfer bzw. das Datenhandling entspricht nicht dem Standard. In Abbildung 2 sind diese Faktoren (0 bis max. 2 Punkte) jeweils separat, aber auch zu einem Gesamtscore (max. 6 Punkte, entspricht dem bestmöglichen Ergebnis) aufsummiert dargestellt, um eine Vergleichbarkeit der bewerteten Apps hinsichtlich der genannten Faktoren zu ermöglichen. Eine explizite Nennung der untersuchten Apps und ihrer Hersteller erfolgt hier nicht, da die gewählten Programme lediglich exemplarisch widerspiegeln sollen, wie entsprechende Medical Apps mit den ihnen anvertrauten Daten umgehen und an welchen Stellen mit Schwachpunkten zu rechnen ist.

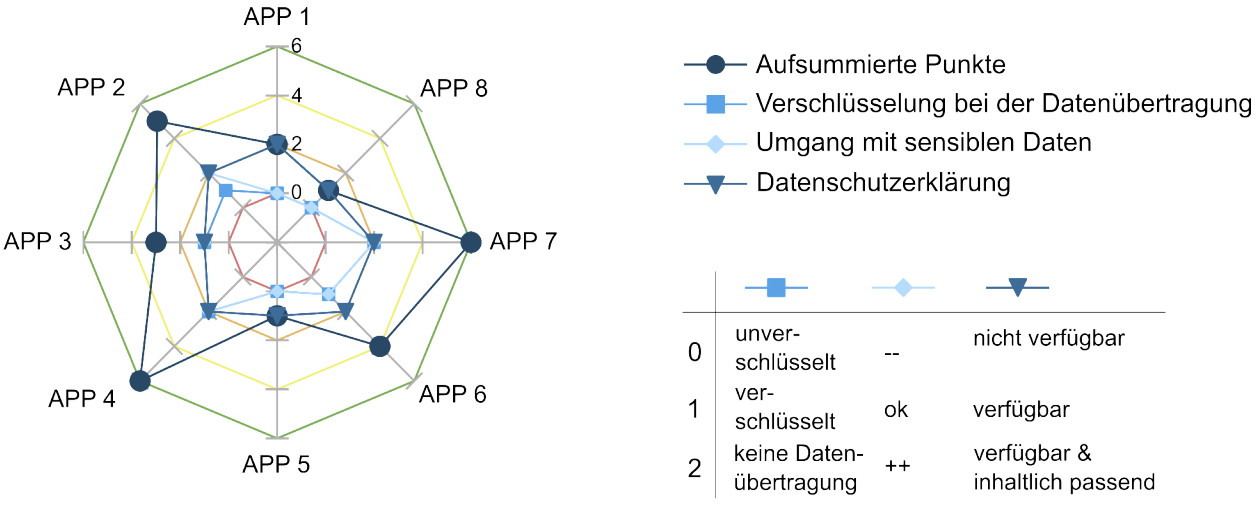

Abb. 2: Bewertung der ausgewählten Applikationen. Die Gesamtbewertung der jeweiligen App ergibt sich aus der Summe der Punkte für die drei Teilbereiche "Verschlüsselung", "Umgang mit sensiblen Daten" und "Datenschutzerklärung"

DETAILS ZU DEN ANALYSIERTEN APPS

Tab. 1: Detaillierte Darstellung der analysierten Apps

App	**APP 1**	**APP 2**	**APP 3**	**APP 4**
Verfügbarkeit	iOS, Android	iOS	iOS, Android	iOS
Kosten	kostenlos	kostenpflichtig (werbefrei)	kostenpflichtig (werbefrei)	kostenlos
Zweck	Blutdruckwerte aufzeichnen und bewerten.	Laborwerte erfassen und erläutern.	Herzfrequenz bestimmen und Werte verwalten.	Blutzuckerwerte erfassen und verwalten; ermöglicht direkten Zugriff auf geeignete Messgeräte.
Score (min. 0 bis max. 6)	**2**	**5**	**3**	**6**
Unverschlüsselte Datenübertragung	ja	Abgesehen von freiwilligem Export der Daten via Email keine Datenübertragung feststellbar.	ja (jedoch nur bei der freien Version zur Kommunikation mit Werbediensten; jegliche weitere Kommunikation geschieht verschlüsselt)	Keine Übertragung der erfassten Daten erkennbar.
Für den Nutzer nicht offensichtliche Datenübertragung	Geräte-ID + und Art des Gerätes	nein	Bei der Kommunikation mit den Werbeservern werden IDs übertragen.	nein
Kommentar	Der Server auf dem die erfassten Daten hinterlegt werden befindet sich in Deutschland. Die Datenschutzerklärung enthält detaillierte Informationen, es werden auch Hinweise zur Vermeidung von unbeabsichtigter Datensammlung gegeben.	Datenschutzerklärung verfügbar und gut an den Zweck des Programms angepasst.	Die Datenschutzerklärung ist nicht speziell auf die App angepasst und deckt alle möglichen Bereiche ab, die nicht unbedingt etwas mit dem Zweck des Programms zu tun haben, z.B. inkl. GPS-Daten. Die Server zur Speicherung der Daten befinden sich in den Vereinigten Staaten und unterliegen damit nur dem dortigen Recht.	Datenschutzerklärung vorhanden und gut auf die Belange des Programms angepasst.

Fortsetzung Tab. 1: Detaillierte Darstellung der analysierten Apps

App	**APP 5**	**APP 6**	**APP 7**	**APP 8**
Verfügbarkeit	iOS, Android	iOS	iOS	iOS
Kosten	kostenpflichtig	kostenlos	kostenlos	kostenlos
Zweck	Stellt Notfallhelfern direkt über das Smartphone medizinische und persönliche Informationen des Anwenders zur Verfügung.	Impfungen erfassen und verwalten.	Erinnert an die Medikamenteneinnahme.	Erfasst und bewertet Vitalwerte; Erfassung kann über geeignete externe Geräte erfolgen.
Score (min. 0 bis max. 6)	**2**	**4**	**6**	**1**
Unverschlüsselte Datenübertragung	ja (alle erfassten Daten inkl. sensibler persönlicher Informationen des Anwenders und seiner im Programm angegebenen Angehörigen).	nein	Keine Übertragung der erfassten Daten erkennbar.	ja
Für den Nutzer nicht offensichtliche Datenübertragung	Geräte-ID und Typ, Spracheinstellung, Zeitzone	Keine versteckte Übertragung erkennbar (Verschlüsselung).	nein	nein
Kommentar	Datenschutzerklärung verfügbar aber nicht gut an den Zweck des Programms angepasst, deckt auch unnötige Bereiche ab.	Datenschutzerklärung verfügbar.	Datenschutzerklärung verfügbar.	Datenschutzerklärung verfügbar.

KRITERIEN ZUR BEURTEILUNG DER DATENSICHERHEIT VON MEDICAL APPS

Die Sensibilisierung der Nutzer über mögliche Datenschutzrisiken im Umgang mit Medical Apps ist ein wichtiger Schritt. Mit diesem Bewusstsein kann auch ohne aufwendige Netzwerkanalyse anhand von einigen einfachen Kriterien, die folgend angeführt werden, eine eigene vorläufige Einschätzung über das Datenschutzniveau der betreffenden App gemacht werden.

Datensammlung und Übertragung

- Sammelt die App offen Daten oder besteht die Gefahr, dass versteckt Daten erhoben und übertragen werden?
- Geschieht die Datenerfassung bzw. Übertragung der erfassten Daten auf freiwilliger Basis, d.h. hat der Nutzer die Chance, die Erfassung oder Übertragung seiner Daten abzulehnen?
- Findet die Übertragung und Speicherung der erfassten Daten auf eine sichere Weise, d.h. nach dem Stand der Technik statt?
- Gibt es Angaben zum Standort des Servers zur Datenspeicherung?

Datenschutzerklärung

- Existiert eine Datenschutzerklärung, die den Nutzer genau informiert ob und wie seine Daten verarbeitet werden und welche Maßnahmen in der App bzw. auf den Servern des Anbieters (falls eine Datenübertragung und externe Datenspeicherung erfolgt) zum Schutz seiner Daten ergriffen werden?
- Deckt die Datenschutzerklärung alle notwendigen Aspekte ab, z.B.
    - den Zweck der Datenerhebung
    - wer Zugriff auf die Daten hat, z.B. inkl. des Anbieters der App bei Verarbeitung von Daten auf dessen Servern
    - wer – außer dem Anwender – potentiell Profit aus den verarbeiteten Daten zieht, z.B. durch statistische Erhebungen, die basierend auf den Daten aller Nutzer durchgeführt werden könnten
    - den Gerichtsstand des Anbieters sowie den Standort der Server auf denen die Daten gespeichert werden; dies hat u.a. Einfluss auf die gesetzlichen Vorgaben, die zum Datenschutz Anwendung finden. Dies ist insbe-

sondere bei Applikationen von Interesse, deren Urheber sich außerhalb Deutschlands oder der EU befinden, da dortige Datenschutzbestimmungen oft nicht das hiesige Schutzniveau erreichen.

- Angabe einer Kontaktadresse und Auflistung der Möglichkeiten, wie ein Nutzer eine Löschung seiner beim Anbieter gespeicherten Daten erreichen kann. Hierbei sollten auch die jeweiligen Löschfristen spezifiziert sein.

Die Einhaltung dieser Kriterien liegt nicht nur im Interesse der Nutzer. Verstoßen Anbieter gegen die genannten Kriterien, riskieren sie, das Vertrauen der Nutzer zu verlieren. Zurzeit werden Entwürfe für Zertifizierungen und das regulatorische Procedere im In- und Ausland diskutiert, um medizinische Apps sicherer zu gestalten.

REFERENZEN

Albrecht UV, Matthies HK, Pramann O. Vertrauenswürdige Medical Apps. In: Reitere H, Deusse O (Hrsg.), Mensch & Computer 2012 – Workshopband: interaktiv informiert – allgegenwärtig und allumfassend!? München: Oldenbourg Verlag. (S. 261-266).

Albrecht UV, Weiss RG, Pramann O. Mobile Anwendungen: Dienstliche Nutzung privater Geräte Dtsch Arztebl 2012; 109(31-32): A-1545 / B-1330 / C-1310.

Pramann O, Gaertner A, Albrecht UV. Medical Apps: Mobile Helfer am Krankenbett. Dtsch Arztebl 2012; 109(22-23): A-1201 / B-1033 / C-1025.

Pramann O, Albrecht UV. Rechtliche Fragestellungen des Einsatzes von Medical-Apps auf mobilen Endgeräten in der Praxis. Tagungsband Telemed 2012, Berlin.

STUDIENDURCHFÜHRUNG

Das PLRI MedAppLab ist eine multidisziplinäre Arbeitsgruppe des Peter L. Reichertz Institut für Medizinische Informatik an der Medizinischen Hochschule Hannover und beschäftigt sich mit ethischen, rechtlichen und praktischen Aspekten des Einsatzes von mobilen Endgeräten im medizinischen Umfeld.

PLRI MedAppLab,
Peter L. Reichertz Institut für Medizinische Informatik der TU Braunschweig
und der Medizinischen Hochschule Hannover,
Medizinische Hochschule Hannover, Carl-Neuberg-Str.1, 30625 Hannover.
URL: www.plrimedapplab.de Email: contact@plrimedapplab.de