App-Monitoring

Allgemeine Informationen

Bei der durchgeführten Analyse bzw. beim Monitoring von Apps geht es darum, die Sicherheit der Datenströme und des Datentransports zu testen, d.h. zu testen, ob die Daten über eine gesicherte **https**-Verbindung laufen. Dies gilt insbesondere für sensible und persönliche Daten, wie etwa Passwörter oder Angaben zum Gesundheitszustand. Zur Analyse der Kommunikation der Apps wird Charles Proxy verwendet.
Erfolgt die Kommunikation über ein http-Protokoll, zeigt dies an, dass die Kommunikation **unverschlüsselt** ist, da das **http-Protokoll** und nicht das **https-Protokoll** verwendet wird. Werden viele Datenströme mit Verwendung eines **http**-Protokolls angezeigt, ist dies ein Anzeichen dafür, dass bei dieser App genauer hingesehen werden sollte. Entscheidend ist dabei konkret die Frage, welche Daten bzw. Kommunikationsvorgänge über eine http-Verbindung transportiert werden. Handelt es sich dabei nur um einfache Bilddateien der Apps, etc. und nicht um personenbezogene Daten, ist dies weniger kritisch und stellt kein größeres Problem dar.
Des Weiteren wird die **Plattform(un-)Abhängigkeit** der Apps analysiert, d.h. es wird einerseits untersucht, ob die Apps grundsätzlich auf den beiden größten App-Plattformen von Apple/iOS und von Google/Android funktionieren und zum Download bereitstehen. Die Ergebnisse dieses Tests können auch von den Angaben der Entwickler und Hersteller mitunter abweichen. Die Analyse zur Sicherheit der Datenströme erfolgt entsprechend auf beiden Plattformen.
Weiterhin wird als drittem Schritt überprüft, ob analysiert werden kann, zu welchem **Standort** insbesondere personenbezogene Daten gesendet werden. Dies ist wichtig, da die IT-Sicherheitsaspekte der Apps mindestens europäischen Recht, besser natürlich noch deutschem Recht genügen sollen. Auf dem Charles-Proxy wird über den Aufruf einer Seite wie bspw. https://geoiptool.com/de/ oder http://www.utrace.de/das Ergebnis ermittelt.

Zudem wird bei den Apps anschließend noch über eine Anti-Viren-Software (etwa von Kaspersky Internet Security) nach potenziell vorhandenen **Bedrohungen** wie Spyware (Spähprogramm, Schnüffelsoftware), Malware (Schadprogramme) oder Viren gesucht. Grundsätzlich lässt sich hierzu noch anmerken, dass bei Apps, welche aus den entsprechenden App-Stores von Google/Apple heruntergeladen werden, Viren/Bedrohungen generell nur ein untergeordnetes Risiko darstellen. „Echte“ Virenscanner sind im App-Store von Apple nicht zu finden, da iOS-Apps nicht die Berechtigung haben, andere Apps zu durchsuchen. Unter iOS sind Sicherheitstools durch das Sandboxing[1] der Gerätesysteme behindert. Dieses Schutzsystem schirmt Apps und das System vor den Zugriffen anderer Apps ab. Ein iOS-Virenscanner kann deshalb das System nicht auf Viren scannen bzw. die Berechtigung erhalten, die Daten anderer Apps zu prüfen bzw. zu scannen.

[1] Sandboxing: iOS-Apps dürfen keinen direkten Zugriff mehr auf Systembestandteile oder andere Programme haben und es ist festgelegt, was die Programme jeweils dürfen. Es gibt die so genannten „Entitlements", das sind bestimmte Zugriffsrechte für Programme. App-Entwickler müssen jeweils angeben, warum die App bestimmte Rechte haben muss, zum Beispiel warum die Apps Zugriff auf Fotos oder Kontakte haben muss.

Des Weiteren werden abschließend noch die Allgemeinen Geschäftsbedingungen (AGB) des jeweiligen App-Herstellers durchgelesen – mit Fokus auf Angaben zum Datenschutz bzw. firmeninterner Umgang von Daten – mit dem Ziel, die zuvor analysierten Ergebnisse mit den Angaben in den AGBs abgleichen zu können und eventuell vorhandene Widersprüche bzw. noch offene Fragen an den Hersteller herausfiltern zu können. Dieser Schritt rundet die Gesamtbewertung ab.

Hinzugefügt werden muss in diesem Zusammenhang, dass über dieses Verfahren und aus rechtlichen Gründen nicht zu erkennen oder herauszufinden ist, was konkret mit den erhobenen Daten passiert bzw. ob der Hersteller die Daten an Dritte weitergibt. Ein Weiterverkauf von den Daten etwa kann nicht bewertet werden. Es handelt sich jedoch insgesamt um ein recht unkompliziertes und nachvollziehbares Verfahren, was auch das Testen von einer größeren Anzahl von Apps ermöglicht.
Nachfolgende Tabelle fasst die seitens ZTG analysierten Kriterien noch einmal zusammen:

Plattformunabhängigkeit/Plattform	
Datentransport verschlüsselt ja/nein (https/http)	
Registrierung	
Benötigte Zugriffsrechte	
Nutzung von Analyse-Diensten (z.B. Google Analytics)	
Analyse der AGB und Datenschutzangaben	
Fazit	

Prüfunterlagen für die Applikation „meinDiabetes“

Auftraggeber: Verlag Kirchheim & Co. GmbH, Kaiserstr. 41, 55116 Mainz

Ansprechpartner: Dr. Katrin Kraatz

Version: Plattform: iOS, Version 1.1.5, 12.07.2018
Android, Version 1.1.4, 10.07.2018

Technische Überprüfung

Plattformunabhängigkeit	„meinDiabetes“ funktioniert sowohl auf iOS als auch auf Android-basierten Geräten. Für iOS ist mindestens die Version 7.0 erforderlich, für Android mindestens die Version 4.0. Die App ist für Smartphones optimiert. Sie läuft auf dem iPad, nicht jedoch auf Tabletts.
Datentransport verschlüsselt ja/nein (https/http)	Der Datenverkehr der App bzw. die Kommunikationsvorgänge werden größtenteils verschlüsselt bzw. über eine https-Verbindung abgewickelt. Es gibt Vorgänge, die via http abgewickelt werden, es handelt sich jedoch um unkritische Daten, bspw. Logos oder Bilder, Lebensmittel aus der Datenbank etc. Bei der Eingabe persönlicher bzw. medizinischer Daten wird https verwendet.
Registrierung	Es ist möglich, dass Nutzer optional ein Konto anlegen können. Im Rahmen der Registrierung werden die erforderlichen Pflichtangaben den Nutzern mitgeteilt. Die eingegebenen Daten in diesem Zusammenhang werden nach Unternehmensangaben zweckgebunden verwendet. Bei Kündigung des persönlichen Nutzerkontos werden die erhobenen bzw. eingegeben Daten in Hinblick auf das Nutzerkonto gelöscht.
Benötigte Zugriffsmöglichkeiten	Die App benötigt Zugriff auf „Fotos/Medien/Dateien“, um bspw. Dateien (Auswertungen etc.) auf Wunsch per Mail zu den behandelnden Ärzten zu senden.
Analyse der AGB und Datenschutzangaben	Innerhalb der App findet sich ein vollständiges Impressum. Datenschutzangaben sind nicht innerhalb der App aufrufbar, sondern erfordern einen Besuch der Webseite des Unternehmens (https://www.diabetes-online.de/datenschutz). Die dort aufgeführten Datenschutzangaben gelten daher auch für die App. Die Datenschutzangaben liegen in deutscher

	Sprache auf der Webseite des Unternehmens vor. In den Datenschutzangaben auf der Webseite wird über die wichtigsten Aspekte wie *„Erhebung, Verarbeitung und Nutzung personenbezogener Daten“, SSL-Verschlüsselung“, „Nutzung von Analysediensten und Cookies“, „Rechte des Nutzers“, „Einwilligung in die Datenverarbeitung“, „Hosting“* und *„Ansprechpartner“* informiert. Das Unternehmen informiert detailliert über die Art, den Zweck und die Dauer der Nutzung der erhobenen personenbezogenen Daten. Nach Angaben des Unternehmens erfolgt keine Übermittlung an Stellen in Drittstaaten. Innerhalb der Datenschutzangaben wird darauf verwiesen, dass bei Fragen zu diesem Themenbereich das Unternehmen über die im Impressum genannte Telefonnummer/E-Mail kontaktiert werden kann. Es wird explizit der Datenschutzbeauftragte mit Angabe einer E-Mail-Adresse genannt. Innerhalb der App wird darauf hingewiesen, dass die Anwendung dieser Applikation keinen Arzt bzw. ärztliche Diagnose ersetzen kann.
Nutzung von Analyse-Diensten (z.B. Google Analytics)	In der App werden die Dienste der etracker GmbH genutzt zwecks Marketing- und Optimierungszwecken. Sie ermöglichen es, unter einem Pseudonym Nutzungsprofile erstellt werden. Hierzu können Cookies eingesetzt werden. Die erhobenen Daten werden jedoch ohne die gesondert erteilte Zustimmung des Betroffenen nicht dazu benutzt, den Besucher dieser Website persönlich zu identifizieren und nicht mit personenbezogenen Daten über den Träger des Pseudonyms zusammengeführt. Der Datenerhebung und -speicherung kann mit Wirkung für die Zukunft widersprochen werden. Nach Herstellerangaben wurde die etracker GmbH mit dem ePrivacyseal EU-Siegel (Gültigkeitsdauer von Februar 2018 bis Februar 2020) der ePrivacy GmbH zertifiziert (https://www.eprivacy.eu/kunden/vergebene-siegel/firma/etracker-gmbh). Eine Nutzung von entsprechenden Analyse-Diensten zur Optimierung einer App ist üblich bei den allermeisten App-Entwicklern.
Fazit	Kein ernsthafter Hinweis für Sicherheitsrisiken. Siegel kann vergeben werden (wünschenswert ist die Implementierung der Datenschutzerklärung in die App).