

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 übertragen werden. 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.

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 natürlich weniger kritisch.

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 fehlerfrei auf verschiedenen Endgeräten funktionieren. 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.

Des Weiteren werden abschließend noch die Allgemeinen Geschäftsbedingungen (AGB) des jeweiligen App-Herstellers analysiert – mit Fokus auf Angaben zum Datenschutz bzw. zur herstellerbezogenen Nutzung der bereitgestellten 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 der Daten etwa kann nicht zweifelsfrei ermittelt werden. Offenkundig wird lediglich, ob die AGBs dies erlauben würden oder ausschließen.

Prüfunterlagen DiaDigital für die Applikation: Omnitest Diabetes Tagebuch

Antragsteller: B.Braun Melsungen AG

Version: iOS Version 1.3.0, 29.10.2018

Android, Version v2.0.0, 29.10.2018

Plattformunabhängigkeit/Plattform	
Datentransport verschlüsselt ja/nein (https/http)	
Nutzung von Analyse-Diensten (z.B. Google Analytics)	
Benötigte Zugriffsmöglichkeiten	
Analyse der AGB/ Datenschutz- /Sicherheitsangaben	

Prüfunterlagen für die Applikation

„Omnitest Diabetes Tagebuch“

Auftraggeber: B. Braun Melsungen AG, Carl-Braun-Straße 1
34212 Melsungen

Ansprechpartner: Markus Wunsch

Version: Plattform:
iOS Version 1.3.0, 29.10.2018
Android, Version v2.0.0, 29.10.2018

Technische Überprüfung

Plattformunabhängigkeit/Plattform	Die App ist für iOS und Android Geräte verfügbar und kann sowohl für Smartphones wie auch Tablets genutzt werden. Die App ist vorrangig für Smartphones optimiert.
Datentransport verschlüsselt ja/nein (https/http)	Die Datenübertragung läuft komplett verschlüsselt via https ab.
Registrierung	Keine Registrierung erforderlich.
Nutzung von Analyse-Diensten (z.B. Google Analytics)	Nutzung der Analytics Technologie des amerikanischen Unternehmens Flurry Inc. (in der Datenschutzerklärung wird darauf hingewiesen), wobei dem Tracking durch den Nutzer widersprochen werden kann. Die Daten werden in pseudoanonymer Form genutzt, d.h. es sollen keine Nutzerdaten weitergegeben werden, die eine Identifizierung des Nutzers erlauben. Grundsätzlich ist die Nutzung von entsprechenden Webanalyse-Diensten bei den meisten gesundheitsbezogenen Apps üblich. Angaben zum Speicherort des Servers von Flurry liegen nicht vor.
Benötigte Zugriffsmöglichkeiten	Wenn die App mit dem Blutzuckermessgerät verbunden werden soll, benötigt die App den Zugriff auf

Prüfunterlagen DiaDigital für die Applikation: Omnitest Diabetes Tagebuch

Antragsteller: B.Braun Melsungen AG

Version: iOS Version 1.3.0, 29.10.2018

Android, Version v2.0.0, 29.10.2018

	<p>Bluetooth. Zudem benötigt die App bei Android-basierten Geräten Zugriff auf den Standort.</p>
Analyse der AGB/Datenschutzangaben	<p>Die Datenschutzerklärung informiert über die Aspekte „<i>Erhebung, Verarbeitung und Nutzung personenbezogener Daten</i>“, „<i>Nutzung von Analysediensten und Cookies</i>“, „<i>Rechte des Nutzers</i>“, „<i>Einwilligung in die Datenverarbeitung</i>“, „<i>Widerspruchsmöglichkeiten</i>“ und „<i>Ansprechpartner</i>“. Nach Herstellerangaben kann der Nutzer die App auch ohne die Eingabe von personenbezogenen Daten nutzen. Ebenso müssen zur vollumfänglichen Nutzung keine personenbezogenen Daten weitergegeben werden; persönliche Daten, die der Nutzer selbst angibt, werden ausschließlich auf dem Endgerät gespeichert. Der Nutzer kann diese Daten jederzeit löschen.</p> <p>Die Nutzungsbedingungen und die Datenschutzbestimmungen sind auf der App sowie auf der Webseite abrufbar und liegen in deutscher Sprache vor. Ein Account muss für die Nutzung der App nicht angelegt werden.</p>
Fazit	<p>Die Verknüpfung der App über Bluetooth verläuft einfach. Die App gibt Anweisungen wie der Nutzer das BZ-Gerät an das mobile Gerät koppeln kann. Das BZ-Gerät ist nach erfolgreicher Kopplung in der App hinterlegt. Nach der jeweiligen BZ-Messung werden die Daten vom BZ-Gerät beim Ausschalten des Gerätes an die App bzw. mobile Gerät übertragen. Zudem lassen sich mehrere Geräte innerhalb der App hinterlegen. Der Nutzer muss jedoch daran denken, die</p>

Prüfunterlagen DiaDigital für die Applikation: Omnitest Diabetes Tagebuch

Antragsteller: B.Braun Melsungen AG

Version: iOS Version 1.3.0, 29.10.2018

Android, Version v2.0.0, 29.10.2018

	Bluetooth Funktion bei der Datenübertragung zu aktivieren.
--	--