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

[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.

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.

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)	
Nutzung von Analyse-Diensten (z.B. Google Analytics)	
Standorte/Speicherorte Nutzerdaten/Analyse-Dienste	
Bedrohungen / Viren	
Analyse der AGB/ Datenschutz-/Sicherheitsangaben	
Fazit	

Prüfunterlagen für die Applikation

„NutriCheck: A-Z Lebensmittel- Nährwerte & Vitamine“

Auftraggeber: Jommi GbR, Merowingerplatz 1, D-40225 Düsseldorf

Ansprechpartner: Fabian Oertel

Version: Plattform: iOS, Version 1.3.0, 18.08.2017

Technische Überprüfung

Plattformunabhängigkeit/Plattform	Die App funktioniert nur auf iOS-fähigen Geräten (kompatibel mit iPhone, iPad, iPod, mindestens iOS 9.0)
Datentransport verschlüsselt ja/nein (https/http)	Der Datenverkehr der App bzw. die Kommunikationsvorgänge werden größtenteils verschlüsselt bzw. über eine https-Verbindung abgewickelt. Datenströme, die nicht über https laufen, betreffen unkritische Daten wie Bilder bzw. Logos und betreffen keine personenbezogenen Datenströme.
Nutzung von Analyse-Diensten (z.B. Google Analytics)	Nutzung von Google Analytics für die Verwendung der App an sich und von Helpshift zur virtuellen Beantwortung von Nutzerfragen (in der Datenschutzerklärung wird ausführlich darauf hingewiesen bzw. erläutert, was der Nutzer darunter zu verstehen hat); der Nutzer hat die Möglichkeit, durch eigene Geräteeinstellungen die Speicherung der Cookies bzw. Textdateien zu unterbinden; hierfür ist ggf. ein gewisses Verständnis der Gerätesoftware notwendig (wenn dies auch potenziell gut zu finden ist); die App ist bei der Verwendung von Google Analytics an die Nutzungsbedingungen bzw. an die Form der Nutzung von Google Inc. angewiesen. Eine Identifizierung des Nutzers durch

	Jommi online ist jedoch nicht gegeben. Grundsätzlich ist die Nutzung von entsprechenden Webanalyse-Diensten bei den meisten Apps aber üblich und Teil der normalen Entwicklungsprozesse.
Standorte/Speicherorte Nutzerdaten/Analyse-Dienste außerhalb von Deutschland/Europa ja/nein	Nein; nur durch Google Analytics erhobene Informationen (über die Cookies) über die Nutzung der Webseite können auf Servern von Google in den USA gespeichert werden (ist jedoch durch die IP-Anonymisierung verhinderbar bzw. auf Server in der Europäischen Union umlenkbar); eine Zusammenführung mit persönlichen Daten durch Google findet nicht statt.
Bedrohungen / Viren	Keine Bedrohungen/Viren gefunden
Analyse der AGB/ Datenschutzangaben	Keine kritischen Passagen bzw. datenschutzrechtlich fragwürdige Aspekte; es wird insgesamt ausführlich über die Datennutzung, -speicherung, und -weitergabe sowie die Lizenzbedingungen informiert. Nach Herstellerangaben müssen zur vollumfänglichen Nutzung keine personenbezogenen Daten weitergegeben werden; bei Ablehnung der Nutzung von Cookies durch Google Analytics können jedoch Nutzungseinschränkungen bei der App entstehen. Weiterhin wird direkt auf den Support durch Jommi hingewiesen, falls es also noch datenschutzrechtliche Fragen geben sollte.
Fazit	Kein ernsthafter Hinweis für Sicherheitsrisiken. Siegel kann daher vergeben werden.