App-Monitoring

1) 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** bzw. in welches Land die Daten bzw. insbesondere personenbezogene 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:

SSiDiary

Plattformunabhängigkeit/Plattform	iOS (nur IPhone; die App kann zwar grundsätzlich auf dem IPad verwendet werden, ist jedoch nicht für dieses Gerät optimiert) sowie Android
Datentransport verschlüsselt ja/nein (https/http)	Die Kommunikationsvorgänge werden sowohl bei iOS als auch bei Android hauptsächlich über https-Protokolle abgewickelt. Die vorhandenen http-Kommunikationsvorgänge betreffen keine sensiblen Daten.
Nutzung von Analyse-Diensten (z.B. Google Analytics)	Nutzung von Google Analytics
Standorte/Speicherorte Nutzerdaten/Analyse-Dienste außerhalb von Deutschland/Europa ja/nein	Nein
Bedrohungen / Viren	Keine Bedrohungen/Viren bei der Android-Version gefunden; gleiches gilt für iOS (siehe Informationen oben)
Analyse der AGB/ Datenschutzangaben	Keine kritischen Passagen bzw. datenschutzrechtlich fragwürdige Aspekte.
Fazit	Kein Hinweis für Sicherheitsrisiken. Siegel kann daher vergeben werden.