

Hannover, 18.08.2021

Pressekontakt

Karina Quentin
Marketing & PR Managerin

press@appvisory.com
Telefon +49 (0)511 20280048
Fax +49 (0)511 35 39 94-12

iOS-Apps und Datenschutz: Zahlen & Fakten

Wie sicher sind iOS-Apps wirklich?

- **68% der Apps nutzen keine verschlüsselten Verbindungen**
- **54% der Apps tracken Nutzer:innendaten**
- **30% der Apps fordern Zugriff auf den Standort**
- **9 von 10 Unternehmen waren 2020 von Cyber-Angriffen betroffen**
- **Statistische Auswertungen zeigen Datenhunger der Apps**

mediaTest digital zieht Bilanz: Die Sicherheitsexperten haben knapp eine Millionen iOS-Appversionen datenschutztechnisch unter die Lupe genommen. Die Ergebnisse verdeutlichen leider: Die Apps nehmen es nicht allzu genau mit dem Datenschutz der Nutzer:innen. Apple verspricht seinen Nutzer:innen zwar absolute (Daten-)Sicherheit, die Ergebnisse sprechen jedoch eine andere Sprache. Viele iOS-Apps weisen zum Teil gravierende Sicherheitslücken und Datenschutz-Verstöße vor.

Hunderttausende iOS-App-Versionen im Datenschutz-Test

Täglich erscheinen hunderte neue Apps in den App-Stores. Die Corona-Pandemie hat diesen Umstand gesteigert und sowohl die Digitalisierung als auch die Ausbreitung von Apps stark vorangetrieben. Um hierbei nicht den Überblick zu verlieren und sich für mobile Datenschutz-Gefahren zu sensibilisieren, erlaubt mediaTest digital einen Einblick in die Datenbank. Der App-Katalog umfasst ca. 900.000 iOS-App-Versionen. Die Auswertung dieser Daten bietet somit eine repräsentative und spannende Übersicht über das Verhalten und den Datenhunger von Apps.

Ergebnisse der Datenschutz-Analyse

Die Auswertung macht deutlich, dass Apple nicht hält, was es verspricht: Die Mehrzahl der iOS-Apps (68%) lassen unverschlüsselte HTTP-Verbindungen zu, indem sie die Verschlüsselung für einige oder alle Verbindungen deaktivieren. 13 Prozent der Apps erlauben generelle unverschlüsselte Verbindungen. Normalerweise sollten mehr als 99 Prozent der Apps verschlüsselt – und somit sicher – kommunizieren. Gleichzeitig haben 24 Prozent ein Problem mit der Certificate Transparency. Das bedeutet, dass diese unsichere Internetverbindungen nicht zuverlässig identifizieren können. Unter Anbetracht der eben genannten potenziellen Sicherheitslücken sind folgende Informationen noch kritischer zu beurteilen. Knapp ein Drittel der Apps (30%) greifen sowohl auf den Standort der Nutzer:innen als auch auf die

Galerie (31%) zu. Und auch auf den Kalender fordert mindestens jede zehnte App den Zugriff an (14%). Auffällig ist zudem, dass 94 Prozent der iOS-Apps Verbindungen in die USA und somit in nicht [DSGVO-konforme Staaten](#) aufbauen. Die Analyse über den AppScan+ ergab für iOS, dass 54 Prozent der Apps potenziell das Mobilgerät der User:innen via AdSupport framework tracken – das heißt in der Lage sind, Nutzungsgewohnheiten, Logindaten und weitere persönliche Informationen zu sammeln. Dieses Framework gewährt den Apps Zugang zu der Werbekennung des Geräts (advertising identifier).

Schützen Sie sich vor mobilen Gefahren!

Die Statistiken zeigen deutlich, dass der Datenhunger der Apps größer ist als viele zunächst annehmen. Insbesondere Unternehmen müssen sich über diesen Umstand bewusst sein und sensible Geschäftsinformationen vor unbefugtem Zugriff und Manipulation schützen. In den Jahren 2020 und 2021 waren bislang neun von zehn Unternehmen von Datenklau, Spionage und Sabotage betroffen. Durchschnittlich verursachte ein Datenverlust dabei 900.000 Euro Schaden. Es empfiehlt sich deshalb der Einsatz einer Mobile-Security-Lösung wie [APPVISORY](#), die iOS-Apps als auch Android-Anwendungen in einer Positiv- und Negativliste (Black- und Whitelist) anordnet und Mitarbeitende unmittelbar über mögliche Risikopotenziale informiert. So haben Unternehmen die Chance, ungewollten Datenabflüssen präventiv aus dem Weg zu gehen.

Der iOS-Appgraph

Die Ergebnisse des Datenschutz-Tests sind in einem übersichtlichen Appgraph visualisiert.

[>> Download Appgraph](#)

Über APPVISORY[®] by mediaTest digital

APPVISORY ist Europas führende App Risk Management-Software. In Verbindung mit Mobile Device Management Systemen oder Stand-Alone stellt die SaaS-Lösung den Schutz sensibler Unternehmensdaten bei der Nutzung mobiler Endgeräte sicher. Mithilfe von APPVISORY setzen Unternehmen ihre individuellen IT-Sicherheitsrichtlinien sowie Vorgaben laut Bundesdatenschutzgesetz (BDSG) und der neuen EU-Datenschutzgrundverordnung (DSGVO) auf allen Mitarbeitergeräten durch.

Gleichzeitig trägt APPVISORY mit seinem App-Client zur Aufklärung und Sensibilisierung der Anwender bei und fördert die Nutzung von Apps und damit die Digitalisierung und Mobilisierung von Geschäftsprozessen. mediaTest digital sichert weltweit betrieblich genutzte Smartphones und Tablets von mehreren Hundert Kunden in der Größe von drei bis 50.000 Endgeräten ab.

12 der größten 25 deutschen Unternehmen sowie zahlreiche mittelständische und kleine Unternehmen aus Wirtschaftszweigen wie Banken, Automotive, Energieversorgung oder Behörden zählen heute zu den zufriedenen Kunden. Das in Deutschland ansässige Unternehmen nutzt ausschließlich deutsche Server für das Hosting und die Entwicklung seiner Lösungen. Mehr Informationen zu APPVISORY finden Sie auf www.appvisory.com.