PRESSEMITTEILUNG

APPVISORY warnt vor Scooter Sharing App „TIER“

- Android-Version mit kritischem Datensendungsverhalten
- iOS-Version besser geschützt
- Offene Schnittstelle ermöglicht Dritten das Tracken von Rollern und Hupen aus der Ferne

Pressekontakt

Karina Quentin |
Marketing Managerin
press@appvisory.com
Telefon +49 (0)511 353 994 22
Fax +49 (0)511 35 39 94-12

Hannover, 14.08.2019

Die Verbreitung der E-Scooter schreitet seit diesem Sommer auch in Deutschland unaufhaltsam voran. In diversen Großstädten wie Berlin, Hamburg, München, Köln oder Hannover erobern die Roller von Sharing-Diensten wie TIER zunehmend das Stadtbild. Doch wie ist es um die sensiblen Daten der Nutzer bestellt, die ihre Rollerfahrten per Smartphone App in Verbindung mit ihrer Kreditkarte oder anderen Zahlungsmitteln durchführen?

Aktuelle Tests der App Security Spezialisten von APPVISORY haben ergeben, dass eine Betriebssystemversion der App „TIER – Scooter Sharing“ höchst kritisches Verhalten an den Tag legt. Zwar sind die Bezahlfunktionen der App in der iOS-Version (3.1.9) als auch in der Android-Version (3.1.6) sicher implementiert, jedoch weist letztere erhebliche Datenschutzmängel auf. So konnte bei der Nutzung die unverschlüsselte Übertragung von Standortdaten, sowohl des Fahrzeugs als auch des Smartphones, nachgewiesen werden. Mithilfe dieser Daten können unbekannte Dritte Bewegungsprofile der Nutzer erstellen. Zudem nutzt die App ein längst verbotenes Tracking-Item, die Android ID, dessen Nutzung seit einigen Jahren von Google offiziell untersagt ist. Der Grund: Sie ist vom Nutzer nur schwer änderbar und lässt so eine Identifikation

der natürlichen Person zu. Auch in puncto Nutzerfreundlichkeit ist die Android-Version im Vergleich zur iOS-Version noch nicht ausgereift.

Deutlich besser sieht es bei der iOS-Variante der TIER-App aus. Hier konnten keine unerlaubten oder unsicheren Verbindungen gefunden werden. Sämtliche übertragenen Daten wie Standortdaten, Kreditkartendaten, Telefonnummer, Name oder Passwort werden allesamt verschlüsselt an die eigenen Server und an die verbundenen Drittanbieter (wie z.B. Segment.io, Adjust oder Telesign) übermittelt. Die jeweiligen Empfänger der Daten werden transparent in der Datenschutzerklärung genannt (https://www.tier.app/privacy-policy/). Somit kann die Nutzung der iOS-Version laut APPVISORY empfohlen werden.

Nutzer sollten sich dennoch im Klaren darüber sein, dass ihre Zahlung samt Kreditkartendaten und Telefonnummer über den US-amerikanischen Bezahlservice „Stripe Inc." (https://stripe.com/de) abgewickelt wird. Dieser wird in der Datenschutzerklärung korrekt ausgewiesen und findet sich sowohl in der iOS- als auch der Android-Variante der App wieder. Darüber hinaus sollte der Nutzer auch wissen, dass nicht nur der Roller selbst per GPS getracked wird, sondern zusätzlich auch das Smartphone des Nutzers. Das Tracking des Smartphones endet jedoch mit Abstellen des Rollers.

Allerdings ist es den Testern gelungen, für die Rollersuche einen beliebigen Standort und Radius anzugeben. Über diesen Umweg lässt sich einfach herausfinden, wo welcher Roller samt Kennzeichen aktuell verfügbar ist. Wenn also beispielsweise ein Stalker wissen möchte, wo eine Person mit einem bestimmten Nummernschild hingefahren ist, muss er nur per Software an jedem beliebigen Gerät beobachten, an welchem Standort dieser Roller wieder als verfügbar auftaucht. Hierbei handelt es sich explizit nicht um ein alleiniges Problem der TIER-Apps, sondern um ein systemisches Problem aller digital gesteuerten, und mit GPS-Modul versehenen Sharing-Fahrzeuge mit Kennzeichen. An dieser wird jedoch Nachholbedarf seitens der Hersteller deutlich, um die besagten Daten nicht so einfach für Dritte zugänglich zu machen. Dass diese Dritten während der Fahrt einen Roller auch hupen lassen können, ist dabei nur ein augenscheinlich unangenehmer Nebeneffekt, der im Straßenverkehr jedoch zu einer ernsthaften Gefährdung werden kann.

Über APPVISORY® by mediaTest digital

APPVISORY ist Europas führende MAM-Software (Mobile Application Management). 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 Bundes-datenschutzgesetz (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.