Fahrzeugdaten

TCS Test: Remote-Apps für Fahrzeuge – Wie sicher sind sie?

„Remote-Apps" für Fahrzeuge liegen im Trend. Dank ihnen können auf Smartphones und Tablets umfangreiche, sogenannt informative Fahrzeugdaten wie Kilometerstand, Tankfüllstand, Serviceintervalle, Reifendruck usw. in Echtzeit ausgelesen werden. Mit solchen Applikationen kann jedoch auch steuernd auf das Fahrzeug zugegriffen werden. Dazu gehören unter anderem das Ver- und Entriegeln des Fahrzeuges und das Schliessen und Öffnen der Fenster. Solche Funktionen sind zwar komfortabel, können jedoch Kriminelle auf den Plan rufen. Die IT-Sicherheit ist somit entscheidend. Der TCS und seine Partnerclubs unterzogen daher drei Remote-Apps (BMW, VW, Renault) einem sogenannten Penetrationstest.

Grundsätzlich sind die drei untersuchten Apps von BMW, Renault und VW sicher und ohne große Risiken nutzbar. Dennoch kann nicht komplett und per se Entwarnung gegeben werden: Alle drei Apps zeigen verschiedene Schwachstellen, die als mittleres Risiko zu bewerten sind und im Extremfall zu einem Fremdzugriff auf das Benutzerkonto und Steuerung aller Remote-Funktionen führen können.
Folgende Schwachstellen wurden im Rahmen der Untersuchung gefunden:

Unverschlüsselte Datenbank

Renault My Z.E. speichert sensible Daten in einer unverschlüsselten Datenbank auf dem Smartphone. Dies ermöglicht Angreifern unter bestimmten Bedingungen, Daten wie zum Beispiel die Fahrzeug-Identifizierungsnummer (FIN) und einen Aktivierungscode auszulesen, mit denen der Angreifer das Fahrzeug auf sich registrieren kann.

Fehlendes Zertifikatspinning

Zusätzlich lässt sich die Verbindung zwischen Renault My Z.E. sowie VW Car-Net und der jeweiligen Cloud unter bestimmten Umständen abhören und verändern. Dies wird einem Angreifer vor allem dann erleichtert, wenn bei dem Gerät des Benutzers bestimmte Sicherheitsfunktionen deaktiviert sind.

Anmeldeinformationen in der URL

Die BMW Connected App kommuniziert mit mehreren Endpunkten in der Cloud. Damit sich der Benutzer nur einmal in der App anmelden muss, werden die Anmeldeinformationen zuerst umgewandelt. Leider wurde eine unsichere Methode für die Übermittlung dieser umgewandelten Anmeldedaten gewählt, sodass ein Account von einem Angreifer unter Umständen übernommen werden kann oder auch sensitive Informationen in den Protokolldateien des Anbieters gespeichert werden, die dort von administrativen Benutzern eingesehen werden können.

Schwache Passwortrichtlinie

Des Weiteren ist in der BMW Connected App eine schwache Passwortrichtlinie implementiert. Die Passwortlänge ist auf eine Mindestlänge von acht Zeichen beschränkt und limitiert zusätzlich die Menge der Sonderzeichen. Dies minimiert die mögliche Stärke des Passwortes, wodurch ein Angreifer leichter Passwörter durch Ausprobieren (sog. Bruteforcing) erraten kann. Auch einfache Passwörter wie zum Beispiel „abcd1234" sind erlaubt. BMW sperrt allerdings nach wenigen erfolglosen Anmeldeversuchen das Benutzerkonto, bis dieses per Mail-Link wieder freigegeben wird.

Fehlende Sitzungsbeendung

Alle drei Apps haben gemeinsam, dass nach einem Logout die Sitzung nicht richtig beendet wird. So kann ein Benutzer einen erfolgreichen Angreifer nicht einfach aussperren.

Fazit

Die drei Apps waren insgesamt sicher nutzbar, dennoch haben sich einige Schwachstellen manifestiert. Das zeigt klar, dass die Hersteller weiter am Thema IT-Sicherheit arbeiten müssen. Mit steigendem Funktionsumfang der digitalen an die Sicherheitsstrukturen größer, wodurch das Thema IT-Sicherheit zukünftig noch mehr als bisher in den Fokus rücken dürfte.

Empfehlungen

- Es sollte die Möglichkeit geben, die Datenübertragung im Fahrzeug komplett zu deaktivieren.
- Die durch den Hersteller gesammelten Daten sollten für den Fahrzeugbesitzer frei einsehbar sein.
- Manche Funktionen, wie die Betätigung der Hupe, sollten aus Sicherheitsgründen während der Fahrt deaktiviert werden.
- Es braucht strengere Passwortrichtlinien.
- Die IT Sicherheitskriterien müssen aktuellen Sicherheitsstandards genügen, idealerweise mit neutralem Nachweis (z.B. Common Criteria).

Tipps für den Konsumenten

- Nicht nur zwischen den Herstellern, auch zwischen den einzelnen Modellen und Ausstattungsvarianten gibt es große Unterschiede im Funktionsumfang der Remote-Dienste. Als Käufer ist es daher immer nötig, die tatsächlich unterstützten Funktionen im Einzelfall zu prüfen.
- Es sollten möglichst sichere Passwörter verwendet werden - bestehend aus Klein- Großbuchstaben, Zahlen, Sonderzeichen und einer Mindestlänge von 12 Zeichen.