Is Your Company Car Exposing Sensitive Data To Hackers?

Insights
11.22.17

In today's world, where lots of sensitive data are stored electronically, prudent companies utilize sophisticated computer cyber security systems to prevent the hacking of such data. They likely also require employees to password-protect their phones and, perhaps, even download security software applications on them for added protection. But how many companies have considered and addressed potential data vulnerabilities posed by company and employee cars? Likely not many, but it appears many should.

According to a recent article published by online magazine Motherboard, cars may be a treasure trove of unsecured data just waiting for a hacker to claim it. A security software engineer discovered that his car's infotainment system did not use modern security software principles, yet it stored a lot of personal data taken from his phone, including call histories, contacts, texts, emails and directory listings from his mobile phone that had been synchronized with his car (using Bluetooth or other connections) and were being stored on the infotainment system in plain text (i.e., unencrypted). Hackers could gain access to this information remotely through car-based internet connections (a growing technology) or directly through the car's USB port. Although mobile operating systems like Google's Android and Apple's iOS have very effective security protections, these protections could be undone by pairing mobile devices to the car's infotainment system.

We don't know how wide-spread this issue is among the various car models manufactured each year, but this revelation should raise several concerns for companies. If employees sync their mobile devices to company car infotainment systems, they could be unknowingly storing personal data in the company car that is susceptible to hackers. In addition, if an employee uses a company-issued or personal mobile device for work, and that device is paired to the company car or even the employee's personal vehicle, sensitive company information (e.g., customer lists and contact info) may be stored in the car and, therefore, vulnerable.

How should companies deal with this apparent security risk? Unfortunately, there are no easy fixes at present. Car manufacturers are just now beginning to discuss how to address data security issues created by their cars. For companies that have a fleet of cars, however, they should contact the car manufacturers to inquire about the security of the cars' firmware (the embedded software). Companies should also keep in touch with their car manufacturers so they can be notified if there are tech-related updates or recalls. If the manufacturer indicates the car's firmware needs updating, ensure this is done as soon as possible, even it means taking the car to the dealership. If

employees are responsible for company car maintenance or if they use their personal cars for work, companies should have a policy requiring employees to update the car's firmware within a set period of time after it becomes available. Companies may also want to consider prohibiting employees from syncing their mobile devices to company vehicles or syncing company-issued mobile devices to their personal vehicles.

In this age of car connectivity, car manufacturers are working on developing more secure systems to protect the data cars collect. Until those systems are a reality, however, companies need to be aware of the data security risks some cars may pose and take whatever steps they can to help reduce that risk.