Sony, Target, Home Depot… Could Your Vehicle be a Hacker's Next Target?

2.10.2015

In this world of connectivity, automobiles become one large mobile device, transmitting and receiving data whether running or not. Whether you are a component manufacturer or a digital provider streaming content into the vehicle, there are new concerns surrounding tracking and hacking that may put American drivers at risk.

The Connected Car's Threat Vectors

The history of hacking the automobile may be relatively new, but has had several illustrious examples in recent months. Hackers have successfully accessed a Toyota Prius, Ford Escape and a Tesla Model S. These hackers disabled the brakes, jerked the steering wheel back and forth, accelerated the vehicle and even turned off the engines. Most recently, the nation was exposed to the risk in a 60 Minutes piece where engineers dialed into a Chevrolet Impala though GM's OnStar system and planted a malicious code that allowed the engineers to control the wipers, horn, throttle and brakes while a helpless Lesley Stahl was at the wheel.

But the concern is more than just taking control of the car. In an interview with CBS This Morning, Senator Ed Markey, D-Massachusetts, commented that manufacturers and content providers "are gathering info about you all the time: where you park, where you drive." As a proponent of a security and privacy rating system, the Senator drew attention to applications that integrate with a vehicle through Bluetooth that could provide malicious code or steal vehicle data. A similar app was recently removed from the Google Play store as a precautionary measure.

The Governmental Response

Related Services

Cybersecurity and Privacy Specialty Team

E-Discovery Specialty Team

Emerging Technology

Media, Entertainment, and Digital Content Law Specialty Team

Privacy, Data Breach & Data Security

Legislators and regulatory agencies have responded, recognizing the threat to vehicles. A February 2015 report notes, “Drivers have come to rely on these new technologies, but unfortunately the automakers haven't done their part to protect us from cyber attacks or privacy invasions. Even as we are more connected than ever in our cars and trucks, our technology systems and data security remain largely unprotected." According to the Detroit News, NHTSA spokesman Gordon Trowbridge stated that the agency is "engaged in an intensive effort to determine potential security vulnerabilities related to new technologies and will work to ensure that manufacturers cooperate and address issues in order to keep motorists safe."

It is likely that the President will take executive action on the cybersecurity front, the legislature will consider new laws on vehicle data, and that NHTSA will take up the regulatory challenge to address these issues in the coming years. Until then, there are a few key approaches every content provider and manufacturer should take.

What Do You Need to Do?

1. Review possible threat vectors, implement security by design and prepare processes to report on hacking incidents.

In Senator Markey’s report, one of the key findings highlighted that most companies in the connected car sector were unaware or unable to report on hacking activities. It is important to understand what threat vectors your business impacts. Are you a content provider that could carry malicious code or a parts manufacturer in the path of a threat vector? Is the data you provide encrypted and can the system detect penetration?

After understanding these threats, companies must have a mechanism or policy in place to report data theft or hacking incidents. The best approach is to create a policy to address the detection, investigation and reporting of any possible incidents.

2. Review your Terms and Conditions to analyze the level of exposure a data breach, data theft or outright hack creates.

Issues with hacking and data breach are only increasing and need to be addressed in your Terms and Conditions. Review your customer’s requirements with an eye towards what potential liability you may have in the case of a data breach and cascade your risk to any vendors who may provide content, code or hardware that may assist in transmitting malicious programs.

3. Learn about the financial and business risks stemming from the threat vectors and cyber-risk.

Not all hacks will be life-threatening. With a wealth of data available in the vehicle and through its content providers, it is possible that hackers will exploit connected vehicle systems. This content, including a driver’s location data and preferences and other data that serves to “improve the driver’s experience” is a treasure-trove to third parties that is often unprotected and an area where drivers cannot opt-out of collection. As seen in recent data breaches, these issues can be costly and

detrimental to business operations.

To better understand the risks, join Butzel Long for a complimentary webinar on cybersecurity and best practices on February 18, 2015.

For more information and to register, *please click here!*