Press Release

Survey: Consumers hold car manufacturers responsible for securing connected vehicles

92% of German respondents think a cybersecurity check should be part of the TÜV main inspection

Hod Hasharon / Munich, May 9, 2019

Most consumers in Germany are concerned about their cars being hacked and expect automobile manufacturers to secure the connected vehicles they produce.

The findings are part of a consumer survey performed by Statista on behalf of Karamba Security in April 2019, which polled 1,000 respondents across Germany. Of those surveyed, 87% said they believe that the responsibility for securing connected vehicles lies with orginal equipment manufacturers (OEMs). In a similar survey carried out by Karamba Security in the United States, only 59% of respondents said the same.

In the German survey, most respondents (80%) stated that their greatest concern is that hackers could hijack the critical safety functions of their automobile, causing malfunctions or accidents that could jeopardize their safety. This is a far higher percentage than those who cited car theft (44%) or data theft (37%) as their greatest fear.

Nearly all respondents (92%) asserted that they believe that security-relevant software should be checked in the TÜV main inspection every two years.

“The survey shows that while consumers are looking forward to the future of autonomous driving, they are clearly concerned about cyberattacks involving their personal safety. This is still the biggest task for the automotive industry to solve,” said Ami Dotan, CEO and co-founder of Karamba Security.

Slightly more than half of respondents (57%) expressed optimism about the future of autonomous driving, and 14% of BMW, Audi, Volkswagen, and Mercedes owners stated that they believe that completely autonomous vehicles will be on the streets in 3-5 years. That said, only 38% stated that they would let their child or grandchild ride in a fully-autonomous vehicle without an override or backup driver.

Embedding security from the start
Cybersecurity is one of the top priorities of the automotive industry and according to Markets & Markets, the global market for automotive cybersecurity will increase from around $1.34 billion in 2019 to $5.77 billion in 2025.

As the market grows, it is imperative that the automotive industry deal forcefully with the cybersecurity threat as vehicles become more connected and more susceptible to cyber attacks.

“When cyberattacks can impact safety, security needs to be built into the vehicle. It should provide realtime prevention of cyber attempts,” continues Rainer Witzgall, Managing Director DACH of Karamba Security. “Our runtime integrity technology assures the software‘s integrity the minute the car leaves the manufacturing plant, leveraging automated Control Flow Integrity (CFI)-patented technology. Self-protecting cars is the only way to go when zero false positives is expected and remediation time can‘t be hours.”

View the full study here.

Resources
Autonomous Security
Karamba Security Approach
Karamba Security FAQ

About Karamba Security
Karamba Security provides industry-leading automotive cybersecurity solutions for autonomous and connected cars. Its Autonomous Security software products, including Carwall and SafeCAN, provide end-to-end, in-vehicle cybersecurity for the endpoints and the internal messaging bus. Karamba Security’s award-winning solutions prevent cyberattacks with zero false positives and secure communications, including OTA updates, with negligible performance impact. Karamba is engaged with 17 OEM and tier-1 customers and has received numerous industry awards. More information is available at www.karambasecurity.com.

Karamba Security Business Contact:
Amir Einav, VP of Marketing
amir.einav@karambasecurity.com
214-620-7320

Media Contact:
PIABO PR
Edith Laga
edith.laga@piabo.de