

# Press Release

8th Allianz Motor Day Digital Live

## Hackers Target Connected Cars

- Allianz calls for European Automotive Security Information Center
- Must be possible to detect and record hacker attacks
- Car accidents after cyberattacks are insured
- Vehicle manufacturers share responsibility if hacker attack causes vehicle malfunction

The 8th Allianz Motor Day, which was broadcast across Europe this September 22, addressed IT security for connected vehicles. Hacker attacks on connected ecosystems are anything but an unrealistic possibility. “Alongside the logistics and energy sector, connected cars may become one of the main targets of IT crime,” said Klaus-Peter Röhler, a member of the Management Board of Allianz SE and CEO of Allianz Deutschland AG.

The number of connected vehicles in Europe is rising fast – from 37 million cars in 2018 to 110 million by 2023\*. And cars will have a special significance in terms of IT security, because their life cycles – from development through production and use to recycling – can last 20 to 30 years. That’s why the key question at the Allianz event was how connected vehicles can be kept secure from cyberattack throughout that whole time.

### Allianz calls for pan-European, multi-industry anti-hacking platform

Mindful of the challenges faced not only by the automotive industry but the insurance sector in dealing with hacker attacks, at its 8th Allianz Motor Day Allianz called for a European solution for a multi-industry **Automotive Security Information Center**.

“We’re facing a threat that doesn’t stop at company walls or national borders, and we believe that such a center must combine data and competencies from multiple institutions, including government agencies, vehicle manufacturers, automotive suppliers, telecommunications operators, research institutions, the repair industry and the insurance industry,” Röhler said.

\*Source: Capgemini 2019

## **Must be possible to investigate cyberattacks**

Another topic at the 8th Allianz Motor Day was accessing vehicle data in the event of a hacker attack. Connected cars must offer adequate protection from potential cyber risks – yet at the same time allow easy, fast access to vehicle data so third parties can develop and propose new products and services to the drivers. In addition to the steps called for at the 2019 Allianz Motor Day for using vehicle data to investigate accidents in connected and smart cars, cyberattacks should also be recorded by an independent data trustee. Such a record could be kept in compliance with the data protection laws, without transmitting personal information. Recording cyberattacks can also serve to improve systems and avert future harm.

## **Damage from hacking is insured in many cases**

Hacker attacks trigger various risk scenarios that are significant for insurers. These include traffic accidents, vehicle thefts, and blackmail after hackers have taken control of the vehicle's systems.

If a cyberattack leads to an accident in which someone is injured, or the driver's own vehicle or someone else's is damaged, the Allianz Group's European subsidiaries generally provide insurance coverage. Third-party damage is covered by vehicle liability insurance; damage to one's own car is included under full-coverage policies. If a hacker attack makes it possible to steal the vehicle, that's included under standard partial-coverage policies in most countries. In Germany, Allianz's full-coverage car insurance policies also include damage to software. "Even if no accident occurs, but the hacker attack damages the software, Allianz has included that damage since last year under its full-coverage policies, provided the hacker attacks the vehicle directly," explained Frank Sommerfeld, CEO of Allianz Versicherungs-AG.

## **Vehicle manufacturers share responsibility if hacker attack disrupts function**

If a hacker attacks vehicle manufacturers servers or digital platforms that communicate with the vehicle, and disrupts functions in multiple vehicles or even all vehicles of a certain type, that's a case for the vehicle manufacturers. It's within the maker's sphere of risk to ensure that the vehicle's electronics remain sustainably functional, and to protect them from attack. That also applies if the attack directly affects the vehicle's functioning.

"But if the functions disrupted by a cyberattack lead to traffic accidents, as the insurer we'd provide coverage if the vehicles involved are damaged or someone gets injured," Sommerfeld said.

## **Allianz's main positions on IT security for connected vehicles:**

- To confront cyberchallenges effectively, Allianz is calling for a European solution for a multi-industry **Automotive Security Information Center**. The center's primary purpose would be to ensure by pooling of competencies that the mobility ecosystem is able to prepare for, and respond to, security

threats, vulnerabilities and incidents, so that everyone involved can best manage their business risks and the risks to customers and third parties.

- Vehicle insurance will cover the consequences of accidents after hacker attacks. But if a vehicle malfunctions and an accident results, the car owner has a right to know whether that was the result of a hacker attack. In addition to the measures called for at the 7th Allianz Motor Day for using vehicle data to investigate accidents in connected and smart cars, future cyberattacks should also be recorded by an independent data trustee. Such records could be kept in compliance with the data protection laws without transmitting personal information. Recording cyberattacks could also serve to develop protective mechanism and avert future damage.
- Vehicle manufacturers are responsible for preventing hacker attacks on their digital platforms that communicate with the vehicle. It's up to the vehicle manufacturers to ensure that vehicles, and especially their automated systems, work without disruption, and to cover the costs of remedying defects. But Allianz will provide benefits for the consequences of accidents, and also for mere disruptions of function in the event of attacks on an individual vehicle.

Munich, September 22, 2020

## **The Allianz Motor Day**

How to give people a chance to experience an insurance company personally? It happens once a year at the Allianz Motor Day – a combination of press conference, series of talks by in-house and outside experts, and an experiential world where all aspects of traffic safety and automotive mobility can be tried out and discussed. Because of the current status of the COVID-19 pandemic, this year the 8th Allianz Motor Day was held for the first time as a digital live event throughout Europe.

You can view and download all press releases, films and presentations from the 8th Allianz Motor Day Digital Live at the Motor Day Web portal, <https://events.techcast.cloud/en/allianz-deutschland/allianz-autotag>

### Contact details:

#### **Allianz Deutschland AG**

Corporate Communications

Christian Weishuber

Telefon: +49 89 3800 18169

Mobil: +49 172 8448464

**Die Einschätzungen stehen wie immer unter den nachfolgend angegebenen Vorbehalten.**

#### **Vorbehalt bei Zukunftsaussagen**

Soweit wir in diesem Dokument Prognosen oder Erwartungen äußern oder die Zukunft betreffende Aussagen machen, können diese Aussagen mit bekannten und unbekanntem Risiken und Ungewissheiten verbunden sein. Die

tatsächlichen Ergebnisse und Entwicklungen können daher wesentlich von den geäußerten Erwartungen und Annahmen abweichen. Neben weiteren hier nicht aufgeführten Gründen können sich Abweichungen aus Veränderungen der allgemeinen wirtschaftlichen Lage und der Wettbewerbssituation, vor allem in Allianz Kerngeschäftsfeldern und -märkten, aus Akquisitionen sowie der anschließenden Integration von Unternehmen und aus Restrukturierungsmaßnahmen ergeben. Abweichungen können außerdem aus dem Ausmaß oder der Häufigkeit von Versicherungsfällen (zum Beispiel durch Naturkatastrophen), der Entwicklung von Schadenskosten, Stornoraten, Sterblichkeits- und Krankheitsraten beziehungsweise -tendenzen und, insbesondere im Kapitalanlagebereich, aus dem Ausfall von Kreditnehmern und sonstigen Schuldern resultieren. Auch die Entwicklungen der Finanzmärkte (zum Beispiel Marktschwankungen oder Kreditausfälle) und der Wechselkurse sowie nationale und internationale Gesetzesänderungen, insbesondere hinsichtlich steuerlicher Regelungen, können entsprechenden Einfluss haben. Terroranschläge und deren Folgen können die Wahrscheinlichkeit und das Ausmaß von Abweichungen erhöhen. Die Gesellschaft übernimmt keine Verpflichtung, Zukunftsaussagen zu aktualisieren.

**Privatsphäre und Datenschutz**

Die Allianz ist dem Schutz Ihrer persönlichen Daten verpflichtet. Mehr dazu [hier](#).