Video-Statement
des Vorstandsvorsitzenden der Allianz Versicherungs-AG
Frank Sommerfeld
zum **8. Allianz Autotag Digital Live**
am **22. September 2020**

Ich begrüße Sie sehr herzlich zu unserem 8. Allianz Autotag in neuem digitalem Gewand. Heute beschäftigen wir uns mit IT-Risiken im vernetzten Ökosystem Auto und damit, wie wir als Versicherer mit diesen neuen Risiken umgehen – deutschland- und europaweit.

Hackerangriffe auf vernetzte Mobilitäts-Ökosysteme sind kein unrealistisches Szenario – im Gegenteil! Es gibt auch schon prominente Beispiele, in denen das Hacken einzelner Fahrzeuge und ganzer Flotten vor und während der Fahrt bereits gelungen ist. Täter waren hier glücklicherweise White-Hat-Hacker, die Sicherheitslücken im System aufdecken und nicht die Absicht haben, Personen zu verletzen.

Noch spielen Cyberangriffe bei der Verursachung von Verkehrsunfällen glücklicherweise keine Rolle. Die Allianz musste noch keinen nachweisbar auf einen Hackerangriff zurückzuführenden Unfall bezahlen. Mit zunehmender Vernetzung und Automatisierung der Fahrzeuge werden Risiken durch Cyberangriffe auf Fahrzeuge jedoch mehr und mehr an Bedeutung gewinnen. In der Versicherungswirtschaft sind diese neuen Risiken weder umfassend noch einheitlich beziffert oder sogar kalkuliert. Nicht in Deutschland und auch nicht in Europa. Um Cyberrisiken für alle Betroffenen kalkulierbar und damit versicherbar zu machen, ist es wichtig, sich mit der IT- und Cybersicherheit vernetzter Fahrzeuge auseinanderzusetzen.

Jede neue Technologie ist mit Risiken behaftet, und jede neue Technologie führt auch zu Schäden. Die Betroffenen hier abzusichern, ist eine wichtige Aufgabe für uns als Versicherer. Bedenken Sie: Viele neue Technologien würde es heute nicht geben, wenn daraus resultierende Risiken nicht erkannt und schließlich durch einen passenden Versicherungsschutz abgedeckt worden wären. Die Grenze der Versicherbarkeit liegt da, wo nicht nur Einzelne betroffen sind, sondern ein Ereignis möglicherweise alle Versicherten betrifft. In der Versicherungswirtschaft sprechen wir

dann von einem Kumulrisiko, bei dem das System der Versicherung nicht mehr funktioniert, da alle Versicherten gleichzeitig einen Schaden erleiden.

Bei Cyberrisiken stellt sich bei vernetzten Fahrzeugen in besonderer Weise die Frage, wo hier die Grenze der Versicherbarkeit liegt. Es ist nicht auszuschließen, dass ein Hacker mit einem Knopfdruck alle Fahrzeuge eines bestimmten Typs angreift. Vergleichbare Risiken sehen wir beim klassischen Computervirus beziehungsweise bei Cyberangriffen auf immobile Systeme wie zum Beispiel Rechenzentren. Wie wir mit diesen neuartigen Risiken umgehen, wollen wir heute auf unserem 8. Allianz Autotag mit Ihnen diskutieren.

Als Versicherer unterscheiden wir im Zusammenhang mit Hackerangriffen verschiedene Risikoszenarien:

1. Hacker manipulieren auf elektronischem Weg das Zugangssystem und die Wegfahrsperre für **einen Diebstahl** des Fahrzeugs.

2. Ein Fahrzeug wird gehackt, und es kommt zunächst nur zu **einer Funktionsstörung,** zum Beispiel, um Lösegeld zu erpressen.

3. Durch einen Hackerangriff wird **ein Unfall** initiiert, der zu Schäden am Fahrzeug, aber auch zu Personenschäden führen kann.

Nicht bloß ein Zukunftsszenario, sondern bereits Realität ist der durch einen Hackerangriff ermöglichte **Diebstahl** eines Fahrzeugs. Dem Hacker gelingt es dabei, Tools zu entwickeln, mit denen der elektronische Schlüssel des Fahrzeugs überwunden werden kann.

Ein weiteres bereits realistisches Szenario sind Hackerangriffe, die **Funktionsstörungen** im Fahrzeug hervorrufen. Die Motive hierfür sind unterschiedlich, teilweise, um Sicherheitslücken aufzudecken, manchmal aber auch, um den Hersteller damit zu erpressen. Die Hacker fordern dann für die Wiederherstellung der Fahrbereitschaft ein Cyber-Lösegeld, wie man es schon aus anderen Industriebranchen kennt.

Die beiden Beispiele bedeuten jedoch „nur“ einen Schaden für das System bzw. für die Hardware sowie entsprechenden technischen und finanziellen Aufwand, um ihn

wieder zu beheben. Dramatisch wird es jedoch, wenn Leib und Leben der Insassen oder anderer Verkehrsteilnehmer in Gefahr gebracht werden, weil aus dem Hackerangriff **ein Unfall** resultiert. Stellen Sie sich vor: Ein Hackervirus übernimmt das System im Auto und suggeriert dem Bremsassistenten ein plötzlich auftauchendes Hindernis. Das Fahrzeug bremst zum Beispiel in voller Fahrt auf der Autobahn ab und verursacht so einen Unfall mit vielen Verletzten und hohem Sachschaden.

Dieses Risiko kann sich dann noch erheblich erhöhen, wenn nicht nur ein einzelnes Fahrzeug von diesem Hackerangriff betroffen ist, sondern es einem Hacker gelingt, alle Fahrzeuge eines bestimmten Fahrzeugtyps gleichzeitig anzugreifen. Und das möglicherweise nicht nur regional in einer Stadt, sondern in ganz Europa oder sogar weltweit.

Wie aber sieht es bei diesen Szenarien mit dem Versicherungsschutz aus? Die gute Nachricht vorweg: Die Versicherung übernimmt fast alle der aufgezeigten möglichen finanziellen Folgen.

Wenn durch einen Hackerangriff ein **Unfall** verursacht wird und Menschen zu Schaden kommen und das eigene oder fremde Fahrzeuge beschädigt werden, besteht generell Versicherungsschutz bei allen europäischen Töchtern der Allianz Gruppe und die Kfz-Versicherung übernimmt die finanziellen Schäden – sie kennt keinen allgemeinen Hacker-Ausschluss. **Die Kfz-Haftpflichtversicherung** ersetzt den Sach- und Personenschaden Dritter oder der eigenen Insassen. Den Fahrzeugschaden am eigenen Fahrzeug ersetzt die **Vollkaskoversicherung**.

Wird durch einen Hackerangriff ein **Diebstahl des Fahrzeugs** ermöglicht, ist dies über die Teilkaskoversicherung in den meisten Ländern, wie in Deutschland, mitversichert.

Etwas differenzierter ist das Bild, wenn es durch einen Hackerangriff lediglich zu einer softwarebedingten **Funktionsstörung** des Fahrzeugs kommt. In **Deutschland** übernimmt die Allianz zusätzlich auch Schäden an der Software. Sie stellt seit einem Jahr die von einem Hacker verursachten Funktionsstörungen den anderen Vandalismusschäden in der **Vollkaskoversicherung** gleich. Wir machen in Deutschland also keinen Unterschied mehr, ob ein Dritter böswillig das Fahrzeug zerkratzt oder ob dieser mittels eines Hackerangriffs die Software des Fahrzeugs

angreift und es auf diese Weise beschädigt. Und die Behebung solcher Störungen kann teuer werden. Wenn das IT-System infiltriert wurde, muss Software neu aufgespielt und bei manchen Fahrzeugmodellen nach Herstellervorgaben eine ganze Reihe von Steuergeräten getauscht werden. Der Kostenaufwand hierfür kann schnell eine Größenordnung von mehreren Tausend Euro erreichen.

Kommt es hingegen zu einem Angriff auf die Server oder die digitale Plattform des mit dem Fahrzeug kommunizierenden **Fahrzeugherstellers**, und resultieren daraus Funktionsstörungen bei mehreren Fahrzeugen oder sogar allen Fahrzeugen eines bestimmten Fahrzeugtyps, ist der Fahrzeughersteller in der Verantwortung. Es gehört zur Risikosphäre des Herstellers, für die dauerhafte Funktionsfähigkeit seiner Fahrzeugelektronik zu sorgen und diese vor Angriffen zu schützen.

Kommt es aber infolge dieser systematischen Funktionsstörungen durch eine Cyberattacke zu Verkehrsunfällen, würden wir als Versicherer dafür aufkommen. Sie sehen – in der Autoversicherung steht der Schutz des Unfallopfers im Mittelpunkt. Wenn es zu Unfällen kommt, Menschen verletzt und Fahrzeuge beschädigt werden, übernehmen wir Versicherer die Schäden.

Auch wenn einige der aufgezeigten Risiken in der Praxis glücklicherweise noch nicht eingetreten sind, sind wir als Allianz fest davon überzeugt, dass Kfz-Versicherungsprodukte in ganz Europa noch umfassender auf diese neuen **kollektiven Cyberrisiken** ausgerichtet werden müssen. Neben komplexen Datenbanken erfordert es dazu vor allem Erfahrung. Um beides auf- bzw. auszubauen, setzen wir zum einen auf eigene technische Untersuchungen in unserem Allianz Zentrum für Technik (AZT) sowie auf weiteren interdisziplinären Austausch mit den Fahrzeugherstellern, den Zulieferunternehmen, der Politik und der Wissenschaft. Das tun wir konsequent, um Risiken und Gefahrenpotenziale rechtzeitig als solche zu erkennen, die Risikoprävention voranzutreiben und eine angemessene Reaktionsfähigkeit auf Schadenfälle herzustellen.

Das Mobilitätsverhalten ändert sich schon heute, neue Konzepte zur Fortbewegung spielen im Rahmen der Planung einer Smart City eine entscheidende Rolle. Autonome Busse und Taxis und fahrerlose Lastenfahrzeuge sind elementare Bestandteile dieser Planungen. Die Menschen werden sich allerdings nur in die Hände automatisiert fahrender oder sogar führerloser Fahrzeuge begeben, wenn sie

darauf vertrauen können, dass die Fahrzeuge ausreichend vor Hackerangriffen geschützt sind und auftretende Schäden übernommen werden.

Ich danke Ihnen für Ihre Aufmerksamkeit und wünsche Ihnen einen spannenden und informativen Allianz Autotag.