Video-Statement
des Vorstandsvorsitzenden der Allianz Deutschland AG
Dr. Klaus-Peter Röhler
anlässlich **des 8. Allianz Autotags Digital Live**
am 22. September 2020

Meine sehr geehrten Damen und Herren,

Ich begrüße Sie sehr herzlich zu unserem 8. Allianz Autotag, der in diesem Jahr erstmalig digital, live und europaweit ausgestrahlt wird. Unser Thema heute: die **IT-Sicherheit in vernetzten Fahrzeugen**.

Auch wenn das Fahrrad an Attraktivität gewinnt, **ist und bleibt das Auto in Europa** weiterhin das **beliebteste Hauptverkehrsmittel**. Geändert haben sich die Eigenschaften moderner Fahrzeuge: waren es früher isolierte Systeme mit Motor, so sind es mittlerweile **Computernetzwerke auf Rädern mit Anschluss ans Internet**. Millionen Zeilen Softwarecodes, Steuergeräte und Sensorik ermöglichen neue Mobilitätskonzepte, hohen Komfort sowie Fahrsicherheit, und ebnen den Weg zum hochautomatisierten Fahren. Und genauso, wie „klassische“ Computernetzwerke zum Ziel von Cyberangriffen werden, sind auch Fahrzeuge zunehmend Cyberrisiken ausgesetzt. Neben dem Logistik- und Energiesektor könnte das vernetzte Auto künftig eines der Hauptziele der IT-Kriminalität werden, denn die Anzahl der vernetzten Fahrzeuge steigt in den nächsten Jahren deutlich an: Allein für Europa prognostiziert das IT-Dienstleistungsunternehmen Capgemini eine **Zunahme von 37 Millionen vernetzte Pkw im Jahr 2018 auf 110 Millionen Fahrzeuge bis 2023**.

Der IT-Sicherheit vernetzter Autos kommt damit nicht nur eine noch größere Bedeutung zu, sie ist auch herausfordernd, denn **Fahrzeuge sind äußerst langlebige Güter.** Der **Lebenszyklus** eines Fahrzeugmodells, von der Fahrzeugentwicklung über den Produktionszeitraum und die Fahrzeugnutzung bis zum Recycling, erstreckt sich **aus Sicht der IT-Sicherheit über 20 bis 30 Jahre**. Das steht in deutlichem Kontrast

- einerseits zur rasanten Geschwindigkeit, mit der sich die Leistungsfähigkeit von Rechnern entwickelt und

- andererseits sich gleichzeitig der Nutzungszyklus der Consumer-Elektronik verkürzt.

Die besondere Herausforderung ist, **zu verhindern**, **dass das Schutzniveau und die Sicherheit** für vernetzte Fahrzeuge durch die Weiterentwicklung der Angriffsmethoden von Hackern **über den Lebenszyklus** der Fahrzeuge kontinuierlich zugunsten der Angreifer **sinkt**. „Sicher“ bedeutet einen angemessenen Schutz vor

- Fahrzeugdiebstählen,
- Schäden am Fahrzeug und
- unbefugte Zugriffe auf Daten, aber insbesondere auch Sicherheit der Insassen und anderen Verkehrsteilnehmer.

Lassen Sie mich nun folgende sechs Aspekte entlang des Lebenszyklus aufgreifen:

1. **Zahlreiche Beteiligte** bei der **Entwicklung** und **Produktion**
2. **Standards** und **Anforderungen** bei der **Zulassung** der Fahrzeuge in Europa
3. **„Security by design“** bei der **Entwicklung** und **nach der Auslieferung**
4. **Sicherer Zugriff** auf die **Fahrzeugdaten**
5. An **nationalen Grenzen** machen Hackerangriffe und Vernetzung nicht Halt
6. **Zukünftiger Handlungsbedarf**

Beginnen möchte ich:

1. Mit der Tatsache, dass es bei der Entwicklung und Produktion hochgradig vernetzter und künftig hochautomatisierter Fahrzeuge **zahlreiche Beteiligte** gibt...

   …und zwar entlang der gesamten Wertschöpfungskette und über den ganzen Lebenszyklus hinweg. Das sind

   - die Abteilungen der Fahrzeughersteller selbst sowie ihre Zulieferer auf allen Ebenen,
   - die Telekommunikationsbranche sowie
   - Softwarefirmen und -entwickler, die an der Produktentstehung ebenso beteiligt sind wie an Services und Produkten, die dann erst im laufenden Betrieb eine Rolle spielen.

Hierbei müssen unzählige digitale Schnittstellen seitens der Hersteller orchestriert werden, die sonst **Einfallstore für Hackerangriffe** öffnen können.

2. **Standards** und **Anforderungen** bei der **Zulassung** der Fahrzeuge in Europa

Aktuell werden **Anforderungen** und **Standards** definiert, die künftig die **Voraussetzung** für eine **Zulassung der Fahrzeuge** auf dem **europäischen Markt** definieren. So hat das „UNECE World Forum for Harmonization of Vehicle Regulations“ im Juni detaillierte Anforderungen an das Management von Cyberrisiken und Software-Updates „Over the Air“ formuliert. Diese werden – voraussichtlich im November 2020 – durch die ISO-Norm 21434 „Road vehicles – Cybersecurity engineering“ ergänzt. Damit kommen auf die Fahrzeughersteller detaillierte Anforderungen in vielen Bereichen zu, unter anderem

- organisatorische Anforderungen und zertifizierte Prozesse sowie
- die Beobachtung und Reaktionsfähigkeit bei Ereignissen über den Produktionszeitraum der Fahrzeuge hinaus.

So wird ein technischer Standard für die Automobilentwicklung geschaffen werden, damit die Einhaltung erwarteter Regelungen bei der Typzulassung von Fahrzeugen nachgewiesen werden kann. Das sind aus unserer Sicht wichtige Schritte in die richtige Richtung. Eine Garantie, dass Fahrzeuge nicht gehackt werden, können sie nicht sein. Aber sie leisten einen wichtigen Beitrag dazu, dass Cyberrisiken minimiert werden.

3. „**Security by design**“ bei der **Entwicklung** und **nach der Auslieferung**

Werfen wir einen Blick auf die technische Sicherheit, die bei der **Entwicklung** eine maßgebliche Rolle spielt, schon **aufgrund der hochgradigen Vernetzung der Fahrzeugkomponenten**. So muss bei 60 und mehr Steuergeräten im Fahrzeug jedes einzelne eine hinreichende Sicherheit gegenüber Manipulationen in seiner spezifischen Anwendung bieten. Können beispielsweise bei einem Steuergerät, welches das Laden und die Leistungsentnahme eines Elektrofahrzeugs kontrolliert, die Software ausgelesen und Parameter verändert werden, so bietet sich ein Einfallstor für unbefugtes Tuning. Dies geht aber mit erheblichen Risiken für eine Überhitzung der Batterie einher und sollte daher unbedingt ausgeschlossen werden.

Aber auch **nach der Auslieferung und Übergabe des Wagens** muss weiterhin die Handlungsfähigkeit in Systemen und der Elektronik gewährleistet werden.

Softwareaktualisierungen durch Over-the-Air-Updates sind heute schon Realität und schaffen Reaktionsfähigkeit für die Softwaresicherheit, wie sie bisher nur beim Besuch einer Werkstatt garantiert werden konnte. Auch die Produktbeobachtung und die Früherkennung von Angriffen im Fahrzeug durch Security-Operations-Center der Fahrzeughersteller müssen künftig einen Beitrag zur Sicherheit vernetzter Fahrzeuge leisten.

4. **Sicherer Zugriff** auf die **Fahrzeugdaten**

Der **sichere Zugriff auf die Fahrzeugdaten** ist entscheidend für ein funktionierendes Mobility Ecosystem, und zwar in „beide Richtungen“:

- das vernetzte Auto muss hinreichenden Schutz bieten vor **Cyberangriffen**
- gleichzeitig aber einen **diskriminierungsfreien Zugriff** auf Fahrzeugdaten erlauben, um so die Entwicklung und Bereitstellung von neuen Produkten und Services auch von Dritten zu ermöglichen.

Letztlich sehr ähnlich wie bei einem Smartphone. Das Betriebssystem ist die Grundlage, aber das reichhaltige Angebot von Apps und Anwendungen machen das Smartphone erst zu dem, was es für den Nutzer darstellt.

Auch wir als Versicherer verstehen uns als festen Bestandteil dieses Ökosystems. Wir haben ein elementares Interesse daran, den **Datenzugriff ausreichend abzusichern** und **praktikable Lösungen mit der Industrie zu erarbeiten**. Auf Basis einer fundierten Risikokalkulation bieten wir Services und Angebote für unsere Kunden wie zum Beispiel Telematik-Tarife an. Dazu gehören digitale Prozesse in der Assistance im Schadenfall von der Erkennung über die Analyse und Bewertung bis zur Abwicklung von Kraftfahrtschäden durch das Smartphone.

Dabei setzt die Allianz stark auf **Prävention** und die **Früherkennung von Schadenszenarien**. Auf der Grundlage der von uns im Allianz Zentrum für Technik erhobenen umfangreichen Daten zu konkreten Schadenfällen tauschen wir uns mit den Herstellern intensiv aus und können so helfen, Entwicklungen rechtzeitig zu erkennen und positiv zu beeinflussen. **Am Beispiel der Fahrzeugentwendung** ist dies gut zu verdeutlichen. Seit mehr als zwei Jahren kann man Fahrzeuge auch mit einem **„Virtuellen Schlüssel“** bestellen. Dieser öffnet, schließt und startet das Auto mithilfe eines Smartphones und ersetzt damit den herkömmlichen Autoschlüssel. Nach einem Diebstahl des Fahrzeuges muss uns der Halter den vollständigen

Schlüsselsatz vorlegen, wenn er seinen Schaden geltend macht. Nur, wie reicht er seinem Versicherer einen virtuellen Schlüssel ein? Wie kann der Kunde nachweisen, dass das Fahrzeug wirklich gestohlen wurde und nicht gerade von einem berechtigten Fahrer genutzt wird, der irgendwann einmal einen virtuellen Schlüssel „bekommen“ hat? Und für den Versicherer stellt sich die Frage – wie und was müssen wir prüfen? Wir haben deshalb federführend mit RCAR, einem Gremium von Automobilforschungszentren aus Europa, Asien, Nordamerika, Südamerika und Australien, einen internationalen **Standard für virtuelle Fahrzeugschlüssel** festgelegt, damit wir unsere Kunden nach einem Totaldiebstahl auch bei der Verwendung eines Virtuellen Schlüssels schnell und komplikationslos entschädigen können. Darüber hinaus setzt der **Standard** zum Schutz unserer Kunden **auch Maßstäbe hinsichtlich der IT-Sicherheit des Gesamtsystems**, das über das Fahrzeug hinaus das Smartphone, das Backend, die Kommunikation und die Nutzinteraktion umfasst.

5. An **nationalen Grenzen machen Hackerangriffe und Vernetzung nicht Halt**

Wir sind davon überzeugt, dass den wachsenden IT-Risiken für vernetzte Fahrzeuge nur durch ein sinnvolles und enges Zusammenwirken aller Beteiligten auf **europäischer Ebene** zu begegnen ist. Wie der Rückruf von 1,4 Millionen Fahrzeugen von Fiat Chrysler nach einer Hackerattacke in 2015 in den USA zeigt, können auch in Europa grenzüberschreitend Tausende von Fahrzeugen von einem einzelnen Angriff betroffen sein. Der finanzielle Schaden dieser Angriffe ist groß. Der Rückruf aller betroffenen Fahrzeuge kostete den Autohersteller 600 Millionen Dollar.

6. Zukünftiger Handlungsbedarf

Angesichts der Herausforderungen, vor denen die **Industrie**, aber auch wir als **Versicherer** bei Hackerangriffen und möglichen europaweiten Kumulrisiken stehen, gibt es in den **folgenden beiden Bereichen** Handlungsbedarf besteht:

1. **Angriffe von Hackern** auf Fahrzeuge und Flotten **müssen künftig schnell und frühzeitig erkannt werden können.** Das betrifft zunächst natürlich die Abwehr der Angriffe, aber auch die Aufklärung möglicher Schäden. Analog zu unseren Forderungen auf dem 7. Allianz Autotag bezüglich der Nutzung von Fahrzeugdaten zur Unfallaufklärung in Deutschland beim automatisierten Fahren ist es aus unserer Sicht erforderlich, **zusätzlich auch Cyberangriffe**

zu erkennen und zu speichern. Eine Speicherung bei einem **unabhängigen Datentreuhänder** könnte – wenn hierbei nur technische und keine personenbezogenen Daten übermittelt werden – datenschutzkonform sowohl den Informationsbedarf der Beteiligten abdecken als auch geeignete Schadenstatistiken ermöglichen, um die Risiken für die Gesellschaft bewertbar und kalkulierbar zu machen.

2. Die schnelle Erkennung und Reaktion auf Cyberangriffe erfordert neben unternehmensindividuellen Lösungen eine **europaweite branchenübergreifende Plattform** für die beteiligten Unternehmen im Mobility Ecosystem. Um den skizzierten Herausforderungen wirkungsvoll begegnen zu können, **fordern wir deshalb auf dem 8. Allianz Autotag eine europäische Lösung für ein branchenübergreifendes „Automotive Security Information Center".**
   Wir haben es mit einer potentiellen Bedrohung zu tun, die weder an Unternehmens- noch an Landesgrenzen haltmacht, und wir sind der Überzeugung, dass ein solches **Center die Kompetenzen verschiedener Institutionen zusammenführen muss**, unter anderem Regierungsbehörden, Fahrzeughersteller, Automobilzulieferer, Telekommunikationsbetreiber, Forschungseinrichtungen, Reparatur- und Versicherungsindustrie. Der primäre Zweck eines Automotive Security Information Center wäre, die Fähigkeit des Mobilitäts-Ökosystems sicherzustellen, sich auf Sicherheitsbedrohungen, Schwachstellen und Zwischenfälle vorzubereiten und darauf zu reagieren, sodass alle Beteiligten ihre Geschäftsrisiken sowie Risiken für Kunden und Dritte am besten bewältigen können. Hier können alle Beteiligten ihre Informationen austauschen, Gefährdungen von dokumentierten Angriffen ableiten und dann Maßnahmen zum gemeinsamen und individuellen IT-Risikomanagement entwickeln. Als **Betreiber** kommen hierfür neben einer öffentlichen Organisation auch privatwirtschaftliche Unternehmen oder Verbände in Betracht. Die gesammelten Informationen zu erkannten und tatsächlichen Vorkommnissen wachsen zu einer **Wissensdatenbank** an. Der Zugang zu solchen Informationen ist nicht nur für die Automobilindustrie wichtig, sondern auch für Wissenschaft, Forschung und Lehre und die Politik. Ein solch interdisziplinärer Austausch an Informationen **fördert Transparenz** und **damit Sicherheit**. Außerdem können ethische Computerhacker,

sogenannte White-Hat-Hacker, so einen weiteren konstruktiven Beitrag zur IT-Sicherheit auch jenseits klassischer Fachkonferenzen leisten. Der Kreis lässt sich außerdem durch institutionalisierte Forensik sowie Versicherungsunternehmen zusätzlich erweitern.

Europa ist heute mitführend, wenn es um die **Entwicklung** und den **Bau** von **Fahrzeugen** geht. Diese Position ist aber nur dann zu halten, wenn wir **auch führend** bezüglich der **IT-Security der Fahrzeuge** und des **gesamten mobilen Ökosystems** sind.