CENTER OF AUTOMOTIVE MANAGEMENT

Prof. Dr. Stefan Bratzel

Automotive Cyber Security

Whitepaper

Eine Studie in Kooperation mit Cisco Systems

Version 1.01 (Stand: 20.12.2023)

Inhaltsverzeichnis

Executive Summary

Im vorliegenden Whitepaper wird argumentiert, dass Cyber Security zu den größten multiplen Herausforderungen der Automobilbranche in den nächsten Jahren zählt. Für Automotive-Unternehmen wird das Thema der „Cyber Security Performance“ zu einem unerlässlichen „Hygienefaktor“.

Mit der zunehmenden Digitalisierung und Vernetzung der Fahrzeuge sowie den Trends der Elektromobilität und des autonomen Fahrens steigt der Bedarf für eine effektive Cybersicherheitspolitik. Gleichzeitig erzeugen jedoch die Kundenwünsche nach „Connected Cars“ und „Connected Services“ einen enormen Wettbewerbs- und Time-to-Market-Druck, bei dem Cyber Security Aspekte in den Hintergrund gedrängt werden können. Hinzu kommt, dass die Umsetzung von Automotive Cyber Security sehr voraussetzungsvoll und komplex ist: Sie umfasst grundsätzlich den gesamten Produktlebenszyklus des Fahrzeugs von der Entwicklung, über die Produktion bis hin zur Fahrzeugnutzung und muss in einer komplexen Wertschöpfungskette mit einer verteilten Verantwortung im großen Lieferanten- und Partnernetzwerk gesichert werden.

Neue regulative Vorgaben zur Cyber-Sicherheit in Kraftfahrzeugen (UN R155 (15) / Verordnung (EU) 2018/858) müssen seit Juli 2022 von den Herstellern in der EU verpflichtend für alle neuen Fahrzeugtypen und ab Juli 2024 auch für alle bestehenden Fahrzeugtypen umgesetzt werden. Die Umsetzung der verschiedenen Standards ist notwendig, aber gleichzeitig folgenreich und aufwendig für die Branche.

Die durchgeführte Meta-Analyse zu den Cyber-Angriffen auf Fahrzeuge und Unternehmen der Automobilwirtschaft offenbart die Dringlichkeit und die stark zunehmenden Risiken. Die Auswertungen der bisherigen Angriffspunkte auf die Cybersicherheit der internationalen Automobilwirtschaft zeigen, dass die Quantität und Qualität der Angriffe in den letzten Jahren erheblich steigt. Die Lieferkette bzw. die komplexe Zuliefererlandschaft gelten als große Schwachstelle und stellen zentrale Angriffspunkte mit einer hohen Eintrittswahrscheinlichkeit und vielfach auch einem hohen Schadensausmaß dar. In einem „Deep Dive“ zur Elektromobilität wird herausgearbeitet, dass die Ladeinfrastruktur für Elektrofahrzeuge zu den besonders gefährdeten Cyber Security Bereichen zählt. Das Lade-Ökosystem ist durch seine verschiedenen Marktteilnehmer außerordentlich komplex und bietet grundsätzlich viele Angriffspunkte für Cyber-Kriminelle. Insgesamt zeigt die Analyse der Cyber-Angriffe, dass das Bewusstsein in der Branche für die Gefahren und Risiken noch deutlich unterentwickelt ist.

Die Entwicklung einer hohen „Cyber Security Performance“ in Automobilunternehmen erfordert große Anstrengungen und muss kontinuierlich überprüft werden. Die auf unterschiedlichen Wertschöpfungsebenen und -stufen der Branche verorteten Unternehmen unterscheiden sich dabei erheblich im Hinblick auf die Qualität der Konzeption und Umsetzung von Cyber Security Programmen. Im Whitepaper wird ein Modell zur empirischen Bewertung der Cyber Security Performance von Automobilunternehmen vorgeschlagen. Das „4C“-Modell vereinigt relevante Leistungskriterien von Cyber Security in vier Dimensionen: Kompetenzen (Competencies), Kooperationen (Cooperations), Kultur & Organisation (Culture & Organisation) sowie die Cyber-Strategie (Cyber Strategy). Dabei wird argumentiert, dass die Erfüllung dieser Cyber Security Kriterien eine wichtige Voraussetzung für eine hohe Leistungsqualität von Cyber Security und damit für den langfristigen Erfolg in den Unternehmen darstellt.

1. Einleitung

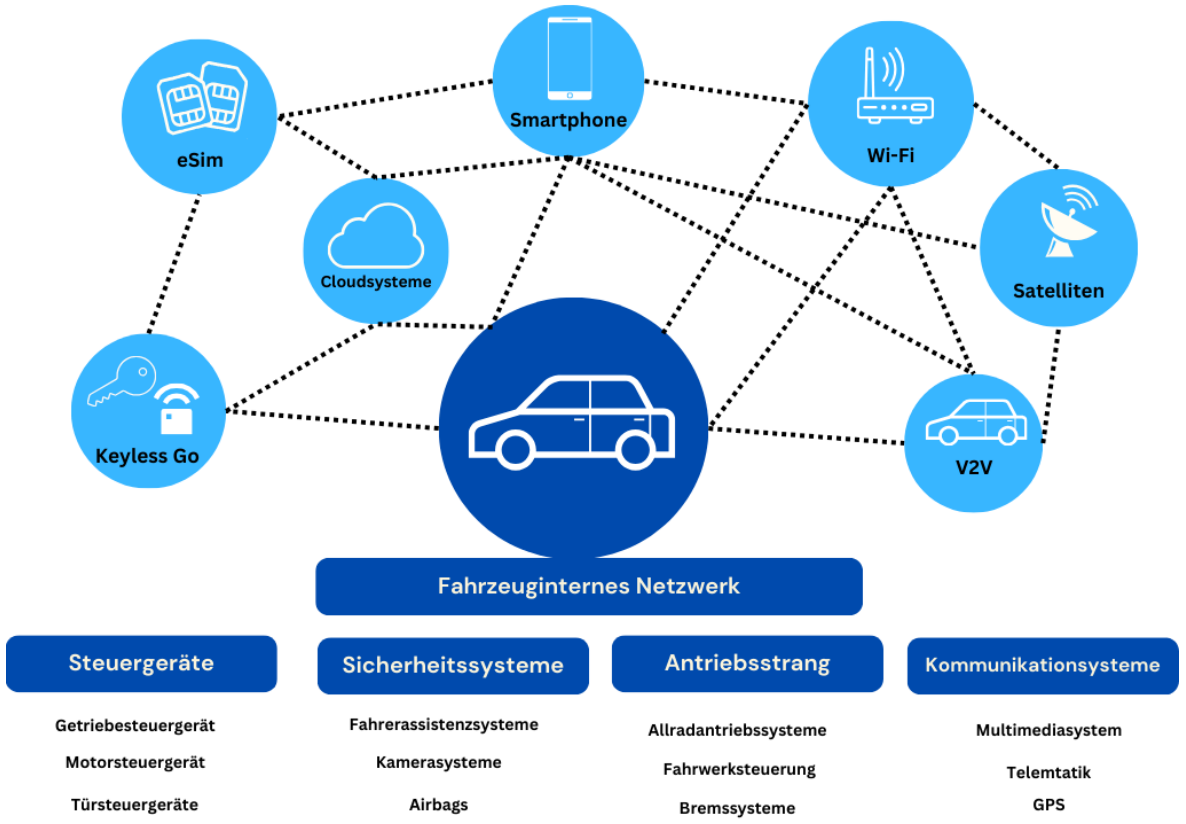
Herausforderungen von Cyber Security in der Automobilindustrie

In der Automobilindustrie steigt mit der zunehmenden Digitalisierung und Vernetzung der Fahrzeuge sowie den Trends der Elektromobilität und des autonomen Fahrens auch der Bedarf an einer effektiven Cybersicherheitspolitik in den Unternehmen. Allein die Zahl der vernetzten Fahrzeuge stieg von 330 Millionen im Jahr 2018 auf rund 775 Millionen im Jahr 2023 (Juniper Research, zitiert in: Global Automotive Cyber Security Report 2022, S. 7). Basierend auf der Daten- und Plattformökonomie durchdringt die Digitalisierung in der Mobilitätswirtschaft die gesamte Wertschöpfungskette der beteiligten Unternehmen (Bratzel/Böbber 2023, S. 18 ff.). Vernetzte Fahrzeuge stellen für die Automobilindustrie dabei einen zentralen künftigen Innovations- und Wertschöpfungspool dar, mit dem sie, z.B. mittels vernetzter Dienste, Over-the-Air (OTA) Software-Updates oder autonomen Fahren, Mehrwerte für ihre Kunden generieren wollen.

Damit steigt das Risiko von Cyberangriffen erheblich. Durch das Sammeln und Verarbeiten großer Datenmengen verschiedener Akteure des Fahrzeugökosystems entstehen viele Angriffspunkte durch zahlreiche mit der Außenwelt vernetzte Sensoren und Steuergeräte im Fahrzeug (Infotainment, V2X, Charging) sowie in den Backend-Servern von Automobilherstellern und Zulieferunternehmen. Mit der Elektromobilität und der zunehmenden Vernetzung der Fahrzeuge (Vehicle-to-X-Kommunikation) steigt die Zahl der Schnittstellen des Fahrzeugs und des automobilen Ökosystems. Dadurch steigen die Angriffsmöglichkeiten exponentiell an (Ladeinfrastruktur, SIM, WLAN, Bluetooth, USB, Funkschlüssel, Diagnoseschnittstelle usw.). Entsprechend sind die Automobilhersteller nicht nur mit der Cybersicherheit des eigenen Fahrzeugs, sondern auch des gesamten Wertschöpfungsnetzwerks konfrontiert. Für Automobile steht die Reduzierung potenzieller Angriffspunkte im Zielkonflikt mit der weiteren Vernetzung des Fahrzeugs und des Angebots von vernetzten Dienstleistungen sowie des autonomen Fahrens

Entsprechend besteht bei allen Akteuren des Fahrzeugökosystems, also Herstellern, Systemlieferanten, KMU‘s sowie weiteren Akteuren des (Lade-)Ökosystems die Notwendigkeit, der Bedrohung von Cyber-Risiken durch entsprechende Strategien und Prozesse zu begegnen.

Abb. 1: Angriffspunkte des vernetzten Fahrzeugs



Quelle: CAM in Anlehnung an Vosseler et al. (2021), S. 4

Definition von Cyber Security in der Automobilindustrie

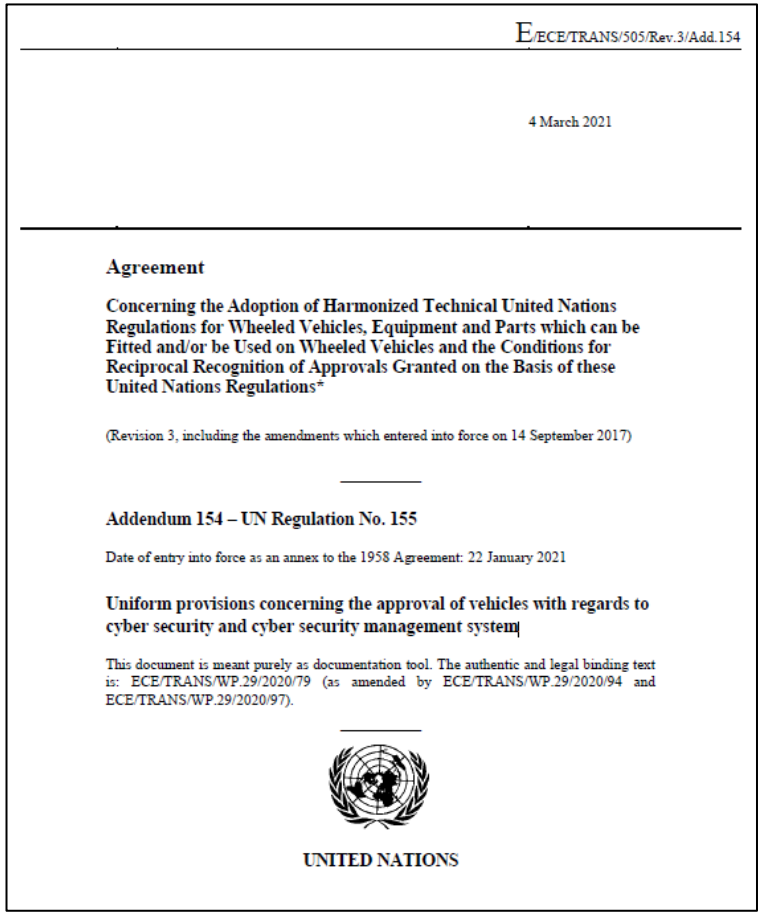
Automotive Cyber Security umfasst die Fahrzeuge inklusive des digitalen Ökosystems sowie den gesamten Produktlebenszyklus.

Cyberangriffe können erhebliche Auswirkungen auf die Sicherheit von Fahrern, Fahrgästen und anderen Verkehrsteilnehmern haben. Cyber Security Governance ist erforderlich, um sicherzustellen, dass Automobilhersteller ihre **Fahrzeuge** vor Cyberangriffen schützen können.
Da die Fahrzeuge jedoch mit den Backend-Servern von Automobilherstellern, mit der externen Infrastruktur (z.B. Ladeökosystemen) oder dem Zuhause bzw. den Endgeräten von Kunden vernetzt sind, umfasst die Cybersicherheit **das gesamte digitale Ökosystem** mit einer Vielzahl von beteiligten Unternehmen. Cyber Security ist dabei nicht nur auf die Nutzungsphase von Fahrzeugen beschränkt, sondern betrifft den gesamten **Produktlebenszyklus**, d.h. die **Fahrzeugentwicklung, Produktion und Fahrzeugnutzung**.

Cyber Security in der Automobilindustrie bezeichnet die Techniken und Maßnahmen, die zur **Vermeidung und zur Abwehr von Cyber-Angriffen auf die Systeme, Netzwerke und Daten von Fahrzeugen** eingesetzt werden. Dazu gehören die Implementierung von Sicherheitsmaßnahmen, die Einhaltung von Sicherheitsstandards, die Überwachung von Datenverkehr und die Bereitstellung von Sicherheitslösungen. Diese Maßnahmen zielen vor allem darauf ab, die Sicherheit von Fahrzeugen und der dahinterliegenden Systeme zu gewährleisten und die Integrität der Daten zu schützen.

> "*Cyber security* means the condition in which road vehicles and their functions are protected from cyber threats to electrical or electronic components." (UNECE 2021: 4)

Abb. 2: UN Regulation Nr. 115



E/ECE/TRANS/505/Rev.3/Add.154

4 March 2021

Agreement

Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations*

(Revision 3, including the amendments which entered into force on 14 September 2017)

Addendum 154 – UN Regulation No. 155

Date of entry into force as an annex to the 1958 Agreement: 22 January 2021

Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

This document is meant purely as documentation tool. The authentic and legal binding text is: ECE/TRANS/WP.29/2020/79 (as amended by ECE/TRANS/WP.29/2020/94 and ECE/TRANS/WP.29/2020/97).

UNITED NATIONS

Quelle: UNECE (2021)

Ziel der Studie und methodisches Vorgehen

Ziel der Studie ist es, den Status sowie die Herausforderungen von Cyber Security in der Automobilbranche zu analysieren und die Leistungsstärke und Qualität des Cyber Security Managements in den Automobilunternehmen belastbar zu vergleichen. Neben der Erhöhung der *Sensibilität* für das Themenfeld ist das indirekte Langfristziel die *Verbesserung der Cyber Security* von Fahrzeugen und von Automobilunternehmen. Die mehrjährige Studienreihe wird von Cisco Systems unterstützt.

Folgende Kernfragen sollen adressiert werden:

- Wie ist der **Status der Umsetzung des Cyber Security Management** (UNECE WP.29 R155 / R156 und ISO/SAE 21434)?
- Welche **Herausforderungen** von Automotive Cyber Security gibt es? Was sind die kritischen Handlungsfelder (Fahrzeug, Back-end, etc.)?
- Was sind die **Qualitäts-/Leistungsmerkmale** von Cyber Security bzw. Cyber Security Management?
- Welche Dimensionen und **Kriterien zur Bewertung der Leistungsstärke** von Automotive Cyber Security sind sinnvoll?

Das vorliegende Whitepaper untersucht im ersten Abschnitt den **State-of-Practice** im Bereich Automotive Cyber Security.

- Dabei stehen zunächst die Standards und das regulative Umfeld des vernetzten Fahrzeugökosystem im Mittelpunkt.
- Danach werden empirische Ergebnisse zu CS-Vorfällen und Angriffen in der Automobilwirtschaft diskutiert.
- In einem Deep Dive wird dann die Cyber Security des automobilen Ladeökosystems diskutiert.
- Am Ende werden die zentralen Herausforderungen und Ansatzpunkte von Cyber Security zusammengefasst.

Im zweiten Abschnitt werden Ansätze und **Kriterien zur Bewertung der Qualität von Cyber Security in Automobilunternehmen** erarbeitet.

- Zunächst wird mit dem „4C“-Modell ein heuristischer Bewertungsansatz vorgestellt, das folgende Dimensionen der Cyber Security Performance adressiert: Competencies, Cooperations, Culture & Organisation, Cyber-Strategy
- Danach wird basierend auf dem Modell erste Elemente eines Befragungskonzepts mit entsprechenden Kriterien und Indikatoren vorgestellt.

Methodisch beruht die Studie auf einer umfassenden Literaturanalyse von empirischen Studien zur Cyber Security in den Automobilbranche. Darüber hinaus wurden Expertengespräche mit hochrangigen Vertretern von Automobilherstellern, Zulieferunternehmen und Verbänden geführt. Außerdem wurden in Expertenworkshops die Ergebnisse reflektiert.

2. State-of-Practice - Cyber Security in der Automobilindustrie

2.1 Standards und Regulation zum vernetzten Fahrzeugökosystem

Das Regulationsumfeld von Automotive Cyber Security

Das Cyber Security-Thema wird bereits von einer Vielzahl von Gesetzen, Regulierungen und Normen begleitet, die sich meist ergänzen.

Die höchste gesetzliche Ebene bilden - vor allem im europäischen Raum - die UNECE-Regulierungen. Hierbei sind die UNECE R-155 für Cyber Security und die R-156 für Software-Updates zu erwähnen. Sie fordern unter anderem die Umsetzung von Managementsystemen und entsprechenden Prozessen zur Sicherstellung der gesetzlichen Anforderungen. Ähnliche Initiativen gibt es in China und USA, wobei dort die UNECE R-155/156 nicht gelten.

Weiter spezifiziert werden die UNECE-Regulierungen durch nationale Gesetze (z.B. nationaler deutscher Gesetzesrahmen zur Umsetzung von SAE-L4-Applikationen).

Darüber hinaus gibt es Normen und Standards, die standardisierte spezifizierte Entwicklungsrahmen, Artefakte und Prozesse anbieten, die es bei einer sicherheitsrelevanten Entwicklung umzusetzen gilt (ISO 21434 Cyber Security oder ISO 20077 Extended Vehicle).

Die Gesetze müssen bei der Entwicklung von sicherheitsrelevanten Kundenfunktionen integriert und über den gesamten digitalen Software-Lebenszyklus gedacht und konzipiert werden. Es ist dabei die gesamte End-to-End (E2E)-Wirkkette zu denken. (vgl. McKinsey 2022; P3 2022: 20-22)

Tab. 1: Überblick einschlägiger (nationaler) Regeln & Vorschriften

(Nationale) Regeln & Vorschriften	Produktsicherheit, (Nationale) Regeln & Vorschriften Haftung & Qualität
UNECE ist aktuell das zentrale Thema für die Homologation und Zulassung. Eine UNECE Zertifizierung ist Grundvoraussetzung für die Zulassung im europäischen und asiatisch/pazifischen (ausgenommen USA China). Für das autonome Fahren relevant sind v.a. folgende UNECEs: - Uniform Provisions Concerning the Approval of: Vehicles with Regard to Steering Equipment (R.79-01) - Cyber Security MS (R.155) - Software Update SUMS (R.156) - Automated Lane Keeping Systems (R.157)	Produktsicherheit umfasst alle konstruktiven Maßnahmen und Aktivitäten, die einen Schaden oder ein Risiko für einen Menschen oder eine Sache verhindern. Das oberste Ziel ist robuste und sichere Produkte herzustellen. Relevante Vorschriften sind: - Funktionale Sicherheit (**ISO 26262**) - SOTIF (**ISO/PAS 21448** oder UL 4600)
Deutschland erlaubt **derzeit** autonome Fahrfunktionen bis SAE-Level 4 (generelle Fahrzeugzulassungen wurden bis zu SAE-L2 gegeben; Stand: 02/21) **US-Zulassungsvorschriften** und Gesetze für autonome Fahrfunktionen **variieren von Staat zu Staat** (max. SAE-L4) – **UNECE gilt nicht** **China** erlaubt derzeit Prototypen-Test bis SAE-L3 & SAE-L4 – eine angepasste ICV Gesetzgebung mit einem erweiterten V2I-Ansatz wird jedoch dieses Jahr in Kraft treten – **UNECE gilt nicht**	Product-Security beschreibt die Fähigkeit, die Nutzung von cyber-physischen Netzwerken vor externen Manipulationen und Attacken zu schützen und zu verteidigen. Automobil-relevante Vorschriften sind: - **ISO 27001** Information Security - **ISO 21434** Automotive Cyber Security - **ISO 20077** Extended Vehicle - **ISO 15408** Evaluation criteria for IT security - **ISO/TR 4804** Safety and Cyber Security for automated driving systems - Software Updates etc.
	Auch die Automobilbranche erfordert eine breite Abdeckung weiterer Normen: - Qualitätsmanagement **ISO 900x/IATF 16949** - Prozessreife **ISO 15504/ASPICE** - Energiemanagement/Umweltmanagement (z. B. **ISO 50001/14001**)

Quelle: P3 (2022), S. 21; CAM

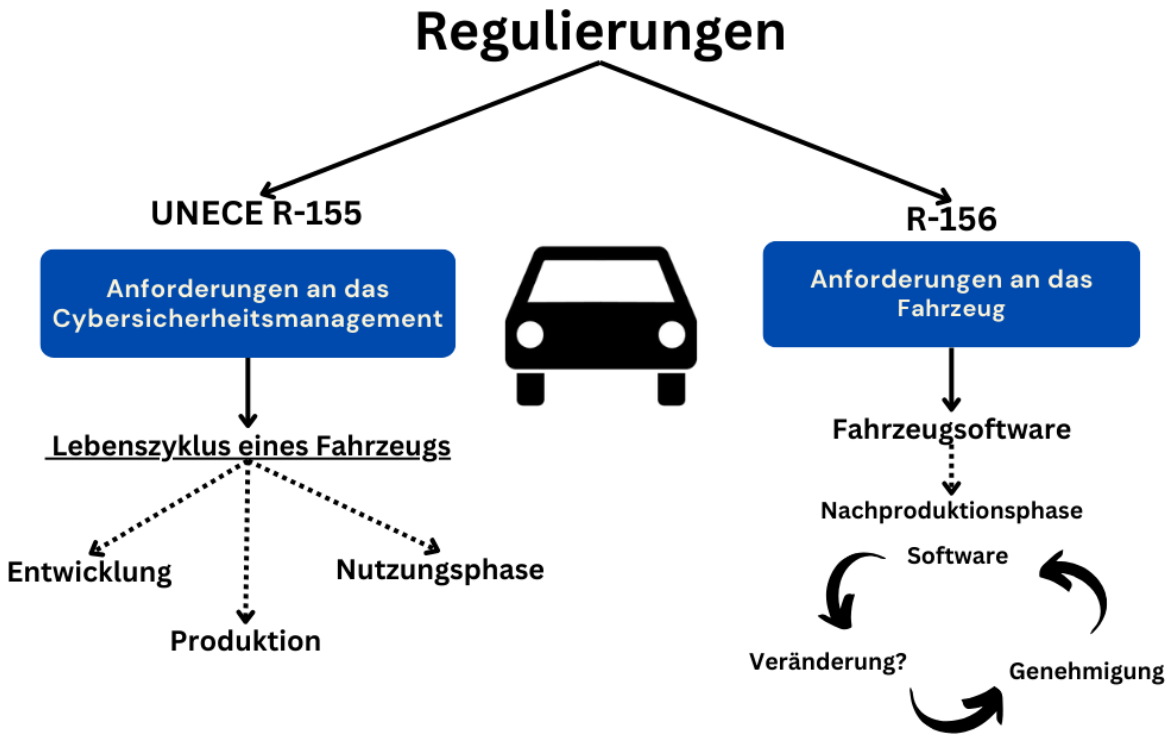
Standards und Regulation zum vernetzten Fahrzeuglebenszyklus

Ein wichtiger Schritt eines einheitlichen Ansatzes zur Adressierung von Cyber Security Risiken sind die im Jahr 2021 verabschiedeten UNECE Regulationen UNECE R-155 (Cyber Security and Cyber Security Management System), UNECE R-156 (Software Update Management System) sowie die Norm ISO/SAE 21434 der internationalen Organisation für Standardisierung. Beide geben zwar keine speziellen Lösungen und genauen Prozesse vor, sondern betonen mittels ihrer Richtlinien, dass CS-Gefahren und Risiken in der Fahrzeugentwicklung, Produktion und im gesamten Fahrzeuglebenszyklus beachtet werden müssen.

Die UN-Regulation für Automotive Cyber Security ist eine internationale Norm, die vom World Forum for Harmonization of Vehicle Regulations (WP.29) erstellt wurde. Sie legt technische Anforderungen an die Cyber-Sicherheit für Fahrzeuge und Systeme fest. Die UNECE R-155 und R-156 gelten in mehr als 50 Ländern als verpflichtende Voraussetzung zur Homologation von Fahrzeugen. Ähnliche Vorschriften sind in den weiteren Kernmärkten USA und China zu erwarten, die sich nicht der UN-Regulation angeschlossen haben. Die UNECE Regulation hat die Automotive Cyber Security in zwei Teilbereiche aufgegliedert:

- Die UNECE R-155 macht Anforderungen für ein Cyber Security Management System (CSMS) eines Automobilherstellers. Berücksichtigt wird der gesamte **Lebenszyklus eines Fahrzeugs** von der Entwicklung, über die Produktion und die Nutzungsphase. Die OEMs müssen auch die Einhaltung der CS-bezogenen Maßnahmen ihrer Automobilzulieferer berücksichtigen.
- Die R-156 Regulation fokussiert auf die **Fahrzeugsoftware** in der Nachproduktionsphase, d.h. eine in der Produktion genehmigte Software muss wiedergenehmigt werden, sofern Veränderungen vorgenommen werden, die die technischen Leistungen beeinflussen.

Abb. 3: UN Cyber Security Regulierungen



"*Cyber Security Management System (CSMS)*" means a systematic risk-based approach defining organisational processes, responsibilities and governance to treat risk.

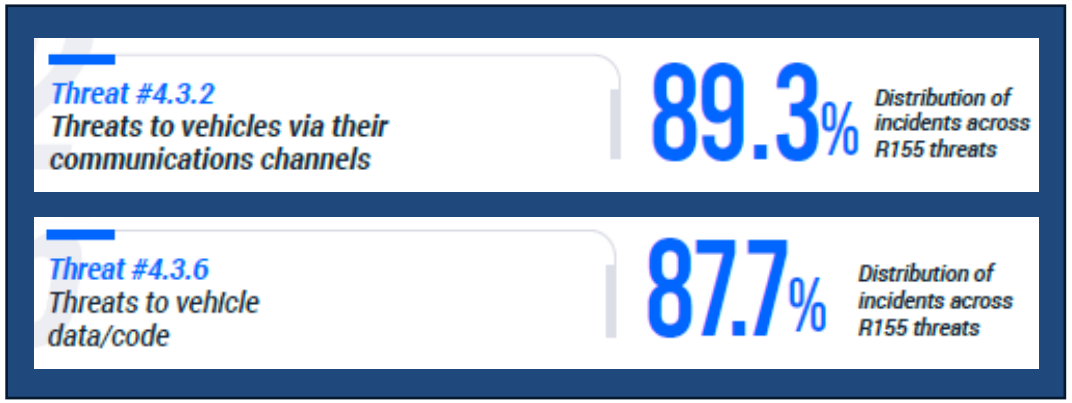
Quelle: CAM in Anlehnung an Zastrow (2022)

Ebenen von Bedrohungen/Verwundbarkeit

Die UNECE Regulation für Automotive Cyber Security identifiziert verschiedene Felder von Bedrohungen bzw. der Verwundbarkeit von Fahrzeugen. Diese beziehen sich u.a. auf Angriffe auf die Backend Server, Kommunikationskanäle, Konnektivität, Software-Updates oder Fahrzeugdaten (vgl. S. 12).

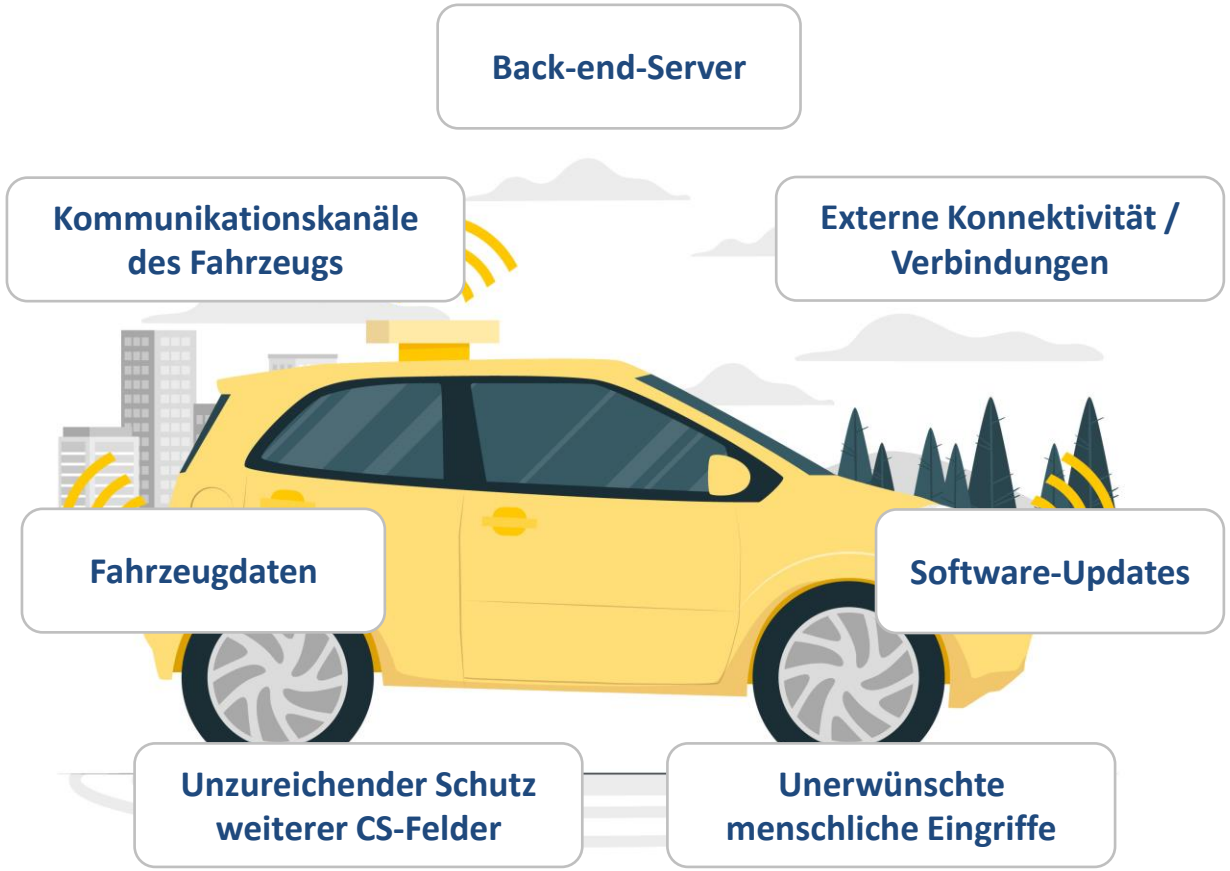
Die empirische Analyse von CS-Vorfällen in der Automobilindustrie in den Jahren 2020/2021 zeigen, dass nahezu 90% der Angriffe über die **Kommunikationskanäle des Fahrzeugs** und im Bereich der **Fahrzeugdaten** stattfinden (vgl. S. 21).

Diese Vorfälle können erhebliche Auswirkungen auf die Vertraulichkeit, Integrität und Verfügbarkeit von Daten bzw. Informationen haben. Die Sicherstellung der Informationssicherheit nach den allgemeinen Grundsätzen (vgl. ISO 27001) ist damit auch Aufgabe des Cyber Security Managements.



Quelle: Upstream (2022)

Abb. 4: Bedrohungsbereiche für Cyber Security Angriffe nach UNECE R-155



Quelle: CAM, Zusammenstellung auf Basis UNECE R-155

Automotive Cyber Security: Ebenen von Bedrohungen/Verwundbarkeit nach UNECE R-155

Abb. 5: Beispiele der Bedrohung/Verwundbarkeit nach UNECE R-155

Back-end-Server	Kommunikationskanäle des Fahrzeugs	Externe Konnektivität / Verbindungen	Software-Updates	Unerwünschte menschliche Eingriffe	Fahrzeugdaten	Unzureichender Schutz / weitere CS-Felder
Unerlaubter Internetzugang zum Server	Eindringen durch Vortäuschen einer falschen Identität („Spoofing“)	Manipulation von Fernsteuerungs- oder Telematikfunktionen (z.B. remote key, charging)	Fehler in den OTA-Update Prozessen, z.B. manipulierte Software wird aufgespielt	Besitzer unterstützt unwissentlich Cyberangriff, z.B. Hochladen von Malware	Entwendung von proprietärer Software oder Daten im Fahrzeug (z.B. Produktpiraterie; Private Nutzerdaten)	Kryptografische Technologien (z.B. unzureichende Verschlüsselung)
Störung von Services, die den Betrieb der Fahrzeuge beeinflussen	Ausführen nicht-autorisierter Veränderungen in den Fahrzeugdaten	Eindringen mittels 3rd Party Software (z.B. Infotainment) oder ext. Interfaces (z.B. USB- oder OBD-port)	Kryptografische Fehler ermöglichen ungültige Updates		Manipulation der Fahrzeugdaten (z.B. Fzg-ID, Fahrdaten, Diagnosedaten)	Hardware oder Software von Zulieferern ermöglicht Angriffe (z.B. Software Bugs)
Datenverlust/-leck	Nicht vertrauenswürdige Informationen werden akzeptiert	Empfang von Nachrichten (z.B. V2V) mit schädlichen Inhalten stören Fahrzeugfunktionen			Fälschen der Parameter für das Laden (z.B. Ladeleistung, Batterietemperatur)	Design von Netzwerken ermöglicht Angriffe (z.B. Überflüssige Internetzugänge)

Verfügbarkeit – Vertraulichkeit – Integrität

Quelle: CAM, Zusammenstellung auf Basis UNECE R-155, Annex 5

Pflichten der Cyber Security nach der UNECE Regulation

Die regulativen Vorgaben zur Cyber-Sicherheit in Kraftfahrzeugen gemäß der UNECE Regelung UN R155 (15) und der Verordnung (EU) 2018/858 müssen seit Juli 2022 von den Herstellern verpflichtend für alle neuen Fahrzeugtypen umgesetzt werden. Im **Juli 2024** unterliegen sowohl alle **neuen als auch alle bestehenden Fahrzeugtypen** der UN R155-Typgenehmigung für Cybersicherheit.

Um die zahlreichen Bedrohungen zu minimieren, fordert die UNECE Regulation (UNECE WP.29 R155) von Automobilherstellern ein funktionierendes **Cyber Security Management System** (CSMS). Er muss zeigen, dass die Prozesse des CSMS die Sicherheit in angemessener Weise berücksichtigen. Daraus ergeben sich **Pflichten zur Definition von organisatorischen Prozessen, Verantwortlichkeiten und Governance des Risikomanagements.**

Gleichzeitig wird eine **umfassende Berichtspflicht** vorgeschrieben, die mindestens jährlich den Genehmigungsbehörden oder dem technischen Dienst vorzulegen ist. Darin sollen auch die Ergebnisse des **Monitorings von Cyberangriffen** und der eingeleiteten Gegenmaßnahmen beschrieben werden. Außerdem besteht nach Art. 33 Abs. 1 DSGVO die **Pflicht zur Meldung**, wenn es erstens eine Verletzung des Schutzes personenbezogener Daten gibt und wenn zweitens diese Verletzung zu einem mehr als nur unerheblichen Risiko für die Betroffenen führt.

Die ab Juli 2024 geltende Anforderung stellt die Automobilhersteller vor große technische und wirtschaftliche Herausforderungen. Als Reaktion hat bspw. Volkswagen bereits bekannt gegeben, dass der VW up! ab Sommer 2024 ohne direkten Nachfolger auslaufen wird. Als Grund werden die hohen Kosten für die Entwicklung einer neuen Elektronik-Architektur genannt, die sich aus wirtschaftlicher Perspektive nicht rentieren würden (vgl. Ecomento 2023). Auch Porsche muss den Macan wegen unzureichender Regelkonformität in der EU frühzeitig vom Markt nehmen. In den USA und China, wo zusammen etwa zwei Drittel des Macan-Absatzes erzielt werden und in denen die UN R155 nicht greift, wird das Fahrzeug weiterhin zum Verkauf angeboten (vgl. Wittich 2023).

Abb. 6: Beispiele für betroffene Fahrzeuge der UN R155

Volkswagen e-up!

Bildquelle: Volkswagen

Porsche Macan

Bildquelle: Porsche

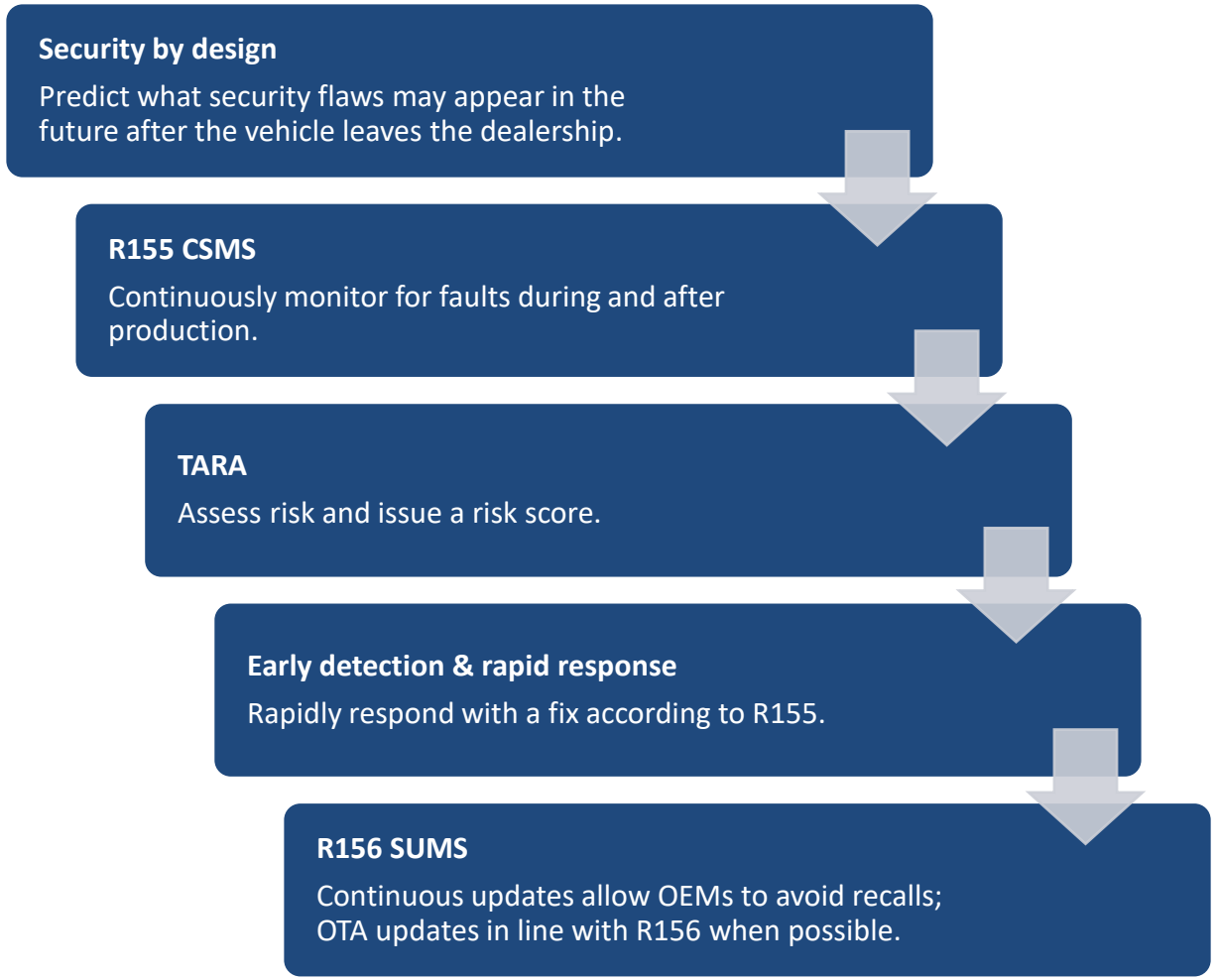
Standard ISO/SAE 21434 als Methodik zur Cyber-Risikoeinschätzung

Im August 2021 wurde der Standard **ISO/SAE 21434 „Road Vehicles Cybersecurity Engineering“** veröffentlicht. Dieser Standard richtet sich an Fahrzeughersteller und definiert einen Rahmen für die Umsetzung von Cyber-Sicherheitsanforderungen in der Entwicklung von Fahrzeugen. Diese bietet eine konkrete Orientierung für die Erfüllung der Zertifizierung zur UN-Regulierung R155. Ein wesentliches Unterscheidungsmerkmal zwischen UNECE WP.29 R155 / R156 Regulation und **ISO/SAE 21434** ist, dass ISO/SAE eine umfassende Methodik bietet, wie OEMs und Tier-Lieferanten **das Risiko von Schwachstellen berechnen**. Der Standard bietet ein strukturiertes Cybersicherheits-Framework, das Cybersicherheit als integraler Bestandteil des Engineerings über den gesamten Lebenszyklus etabliert.

„Die Aktivitäten in der Produktentwicklung nach Norm werden auf Basis einer Risikoeinschätzung gesteuert. Dazu werden Maßnahmen zur organisatorischen Verankerung gefordert. Prozesse werden zwar gefordert, die Norm beschreibt jedoch nur jeweils die Aufgabe eines Prozesses und überlässt die Gestaltung des Ablaufs den Unternehmen. Spezielle Technologien oder Lösungen werden nicht vorgeschlagen.“ (…) (Wikipedia 2023)

„Derzeit in Entwicklung befindet sich der Standard ISO/DIS 24089 „Road Vehicles – Software Update Engineering“. (…) Der ISO 24089 soll die Umsetzung der regulatorischen Anforderungen aus der UNECE Regelung UN R156 unterstützen. Auch dieser Standard sieht eine explizite Betrachtung von Cyber-Sicherheitsrisiken im gesamten Update Prozess vor.“ (BSI (2022), S. 23)

Abb. 7: ISO/SAE 21434, R155 und R156 in der Praxis



Quelle: CAM in Anlehnung an Upstream (2022), S. 17

Integrierte Perspektive im Entwicklungsprozess wichtig: Security + …

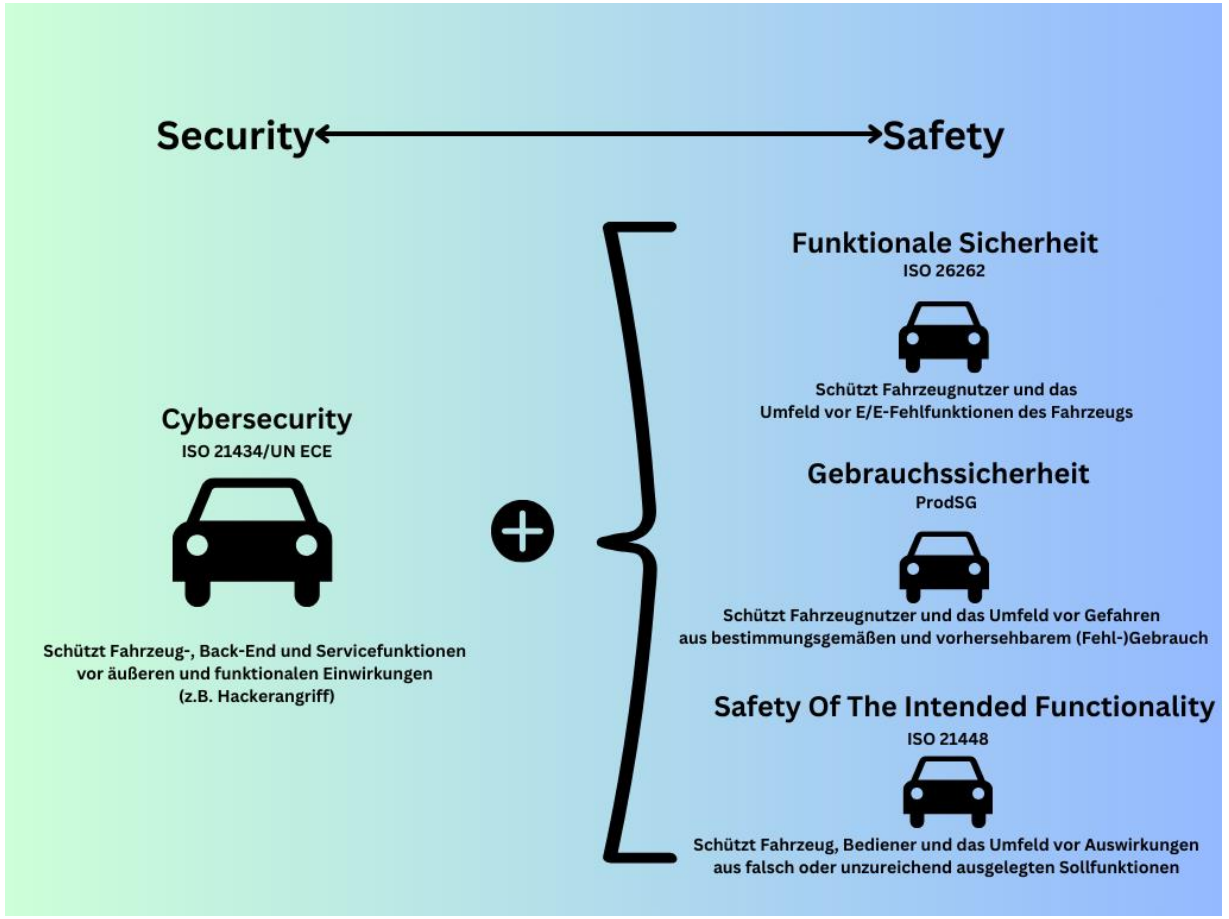
Die Entwicklungsprozesse für Cyber Security (Security) gem. ISO 21434 und die funktionale Sicherheit (Safety) gem. ISO 26262 (sowie idealerweise für Gebrauchssicherheit und SOTIF gem. ISO 21448) müssen entsprechend eng miteinander verzahnt gedacht werden, um das gemeinsame Ziel eines sicheren E/E-Systems und Gesamtprodukts effektiv zu erreichen. Es ist also eine **integrierte Betrachtung *im Entwicklungsprozess*** wichtig, um ein sicheres E/E-System und Gesamtprodukt zu erreichen!

- **SECURITY** (Cyber Security ISO 21434/UNECE): Schützt Fahrzeug-, Back-End und Servicefunktionen vor äußeren und funktionalen Einwirkungen (z.B. Hackerangriff)

  +

- **SAFETY (Funktionale Sicherheit** ISO 26262): Schützt Fahrzeugnutzer und das Umfeld vor E/E-Fehlfunktionen des Fahrzeugs
- **Gebrauchssicherheit**(ProdSG): Schützt Fahrzeugnutzer und das Umfeld vor Gefahren aus bestimmungsgemäßen und vorhersehbarem (Fehl-)Gebrauch
- **Safety Of The Intended Functionality** (**SOTIF) (**ISO 21448 (CD)): Schützt Fahrzeug, Bediener und das Umfeld vor Auswirkungen aus falsch oder unzureichend ausgelegten Sollfunktionen

Abb. 8: Relevanz der Perspektive im Entwicklungsprozess



Quelle: CAM in Anlehnung an P3 (2022), S. 27

ISO/SAE 21434: Bedrohungsanalyse und Risikobewertung

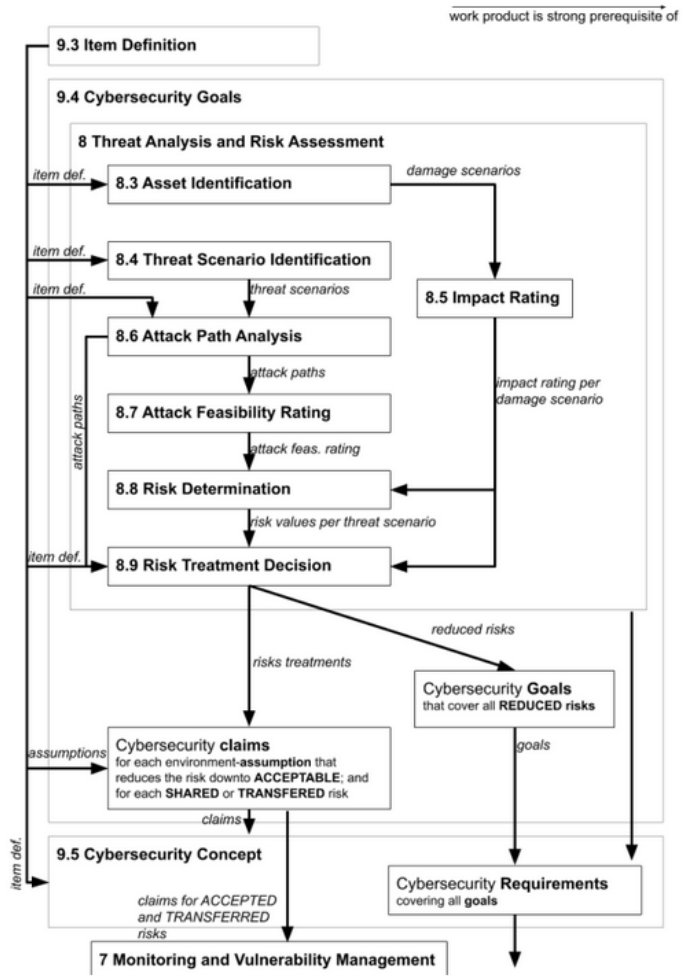
Die technische Risikobetrachtung betrifft die **Schwere der möglichen Auswirkung** und die **Eintrittswahrscheinlichkeiten**, dabei werden Hazard and Risk Analysis (HARA) und die Threat And Risk Analysis (TARA) unterschieden.

Ein zentraler Punkt der ISO/SAE 21434 („Road Vehicles Cybersecurity Engineering“) ist entsprechend die **Bedrohungsanalyse und Risikobewertung**. ISO 21434 unterscheidet drei Arten von Produktphasen: Konzeptphase, Entwicklungsphase und Betriebsphase. Der Hauptteil der Identifizierung von Cybersicherheitszielen besteht darin, die TARA (Threat And Risk Analysis) aufzurufen (Kapitel 8).

Die Hauptschritte bei der Durchführung einer ISO/SAE 21434-konformen Bedrohungsanalyse und Risikobewertung sind (in der Reihenfolge einer idealisierten linearen Ausführung) (vgl. itemis SECURE (2023)):

- Item-Definition (Abschnitt 9.3)
- Asset-Identifizierung (Abschnitt 8.3)
- Identifizierung von Bedrohungsszenarien (Abschnitt 8.4)
- Schadens-Bewertung (Abschnitt 8.5)
- Angriffspfadanalyse (Abschnitt 8.6)
- Bewertung der Durchführbarkeit eines Angriffs (Abschnitt 8.7)
- Risikobestimmung (Abschnitt 8.8)
- Entscheidung zur Risikobehandlung (Abschnitt 8.9)
- Ziele der Cybersicherheit [RQ-09-07]
- Cyber-Sicherheitsansprüche [RQ-09-08]
- Cyber-Sicherheitskonzept (Abschnitt 9.5)

Abb. 9: Bedrohungsanalyse ISO/SAE 21434



Quelle: itemis SECURE (2023)

Risiken und Angriffspunkte im Produktlebenszyklus der Automobilwirtschaft

Die Automotive Cyber Security umfasst grundsätzlich den Produktlebenszyklus des Fahrzeugs von der Entwicklung, über die Produktion bis hin zur Fahrzeugnutzung.

Die verschiedenen Phasen den Produktlebenszyklus bergen unterschiedliche Angriffspunkte und Risiken:

1. Entwicklung
Hohe Bedeutung und CS-Risiken aufgrund breiter Angriffsmöglichkeiten und vieler Schwachstellen, u.a auch im von Zuliefernetzwerk

2. Produktion
Mittlere Bedeutung und CS-Risiken

3. Fahrzeugnutzung
Sehr hohe Bedeutung und CS-Risiken

Abb. 10: Risiken im Produktlebenszyklus der Automobilwirtschaft

Entwicklung

Hohe Bedeutung/Risiken +++

- Entwicklung ermöglicht Zugriff auf Hardware und Software eines Fahrzeugs (breite Angriffsmöglich-keiten; potenziell hohe Zahl betroffener Fahrzeuge/hohes Schadensausmaß)
- Fahrzeugentwicklung begünstigt Schwachstellen (z.B. Verschlüsselung, Fehler im Code, Software von Drittanbietern)
- Gute Sicherung der Entwicklungsbereiche bei OEM / breite Test-/Iterationsprozesse
- Gefahr der gezielten Informationsbeschaffung über Angriffspunkte von Fahrzeugen für spätere Angriffe
- Sicherheit der Unternehmensnetzwerke zentral

Produktion

Mittlere Bedeutung/Risiken ++

- physische Zugriff auf Fahrzeuge und/oder deren Steuergeräte durch Unbefugte (gezielte Manipulation)
- Unbeabsichtigte Fehler: z.B. Angriffe über offene Fahrzeugschnittstellen in der Produktion (OBD-Software, Einspielen von Malware)
- Einbau manipulierter Bauteile/Steuergeräte
- Durch Regulation/Standards für Software soll sichergestellt werden, dass nur homologierte Software aufgespielt wird (siehe UNECE R-156)

Fahrzeugnutzung

Sehr hohe Bedeutung/Risiken ++++

- Dauer von SW-Updates für CS der Fahrzeugflotten noch ungeklärt
- Identifizieren von Schwachstellen, z.B. anhand öffentlicher Quellen, z. B. der CVE-Datenbank des National Institute of Standards and Technology
- Etablieren von Organisationen/ Strukturen der Fahrzeugüberwachung
- Angriffe über die zahlreichen Kommunikationsschnittstellen (Mobilfunk, WLAN, etc.) und Anwendungen (V2X)
- Typische Angriffspunkte:
  - Backend-Server
  - Fahrzeugkommunikations-schnittstellen
  - SW-Update-Verfahren
  - Externe Konnektivität
  - Fahrzeugdaten/-code
  - Mangelnde Systemsicherheit
  - Unbeabsichtigtes menschliches Handeln
- Durch Variantenvielfalt und Software-Updates im Lebenszyklus steigt die Anzahl im Feld befindlicher Fahrzeugkonfi-gurationen exponentiell und erschwert CS

Quelle: CAM in Anlehnung an P3 (2022), S. 14-18

2. State-of-Practice - Cyber Security in der Automobilindustrie

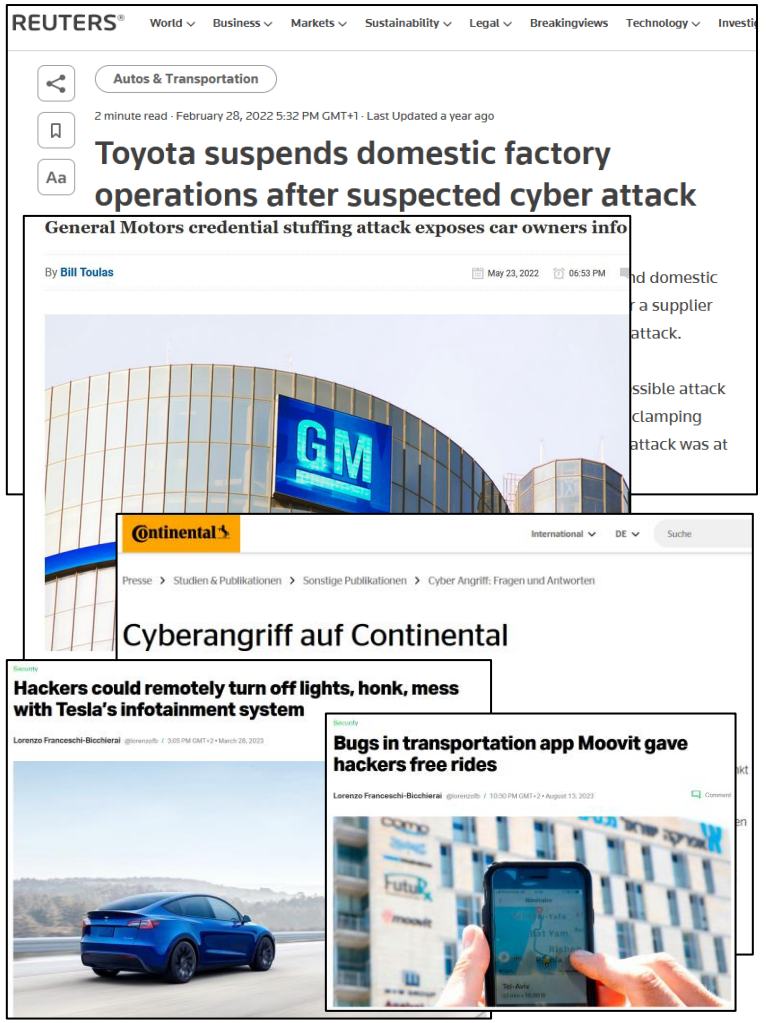
2.1 Standards und Regulation zum vernetzten Fahrzeugökosystem

2.2 Empirische Erhebungen zu CS-Vorfällen und Angriffen in der Automobilwirtschaft

Cyber-Angriffe auf die Automobilindustrie: Internationale Beispiele (1)

- Mittels einer **Meta-Analyse** werden nachfolgend Studien zu den Cyber-Angriffen auf Fahrzeuge und Unternehmen der Automobilwirtschaft ausgewertet. Beispiele von aktuellen Cyber-Angriffen auf Auto-mobilunternehmen zeigen dabei die **Dringlichkeit und Bedeutung** des Themas. Gleichzeitig offenbaren die Auswertungen auch die **bisherigen Angriffspunkte** auf die Cyber-Sicherheit der internationalen Automobilwirtschaft.
- Aus der Meta-Analyse werden Schlussfolgerungen zu den Cyber-Angriffstrends in der Automobilwirtschaft und der Herausforderungen abgeleitet.
- Aktuelle Beispiele auf die Automobilindustrie aus den Jahren 2022/2023 zeigen, dass die gesamte Branche betroffen ist:
  - Nachdem ein Zulieferer von Kunststoffteilen und elektronischen Komponenten von einem mutmaßlichen Cyberangriff getroffen wurde, musste **Toyota** im Februar 2022 den Betrieb seiner japanischen Fabriken kurzzeitig aussetzen und konnte rund 13.000 Autos nicht planmäßig bauen.
  - Der US-Hersteller **General Motors** gab bekannt, dass er im April 2022 Opfer eines Cyber-Angriffs wurde, bei dem einige Kundendaten preisgegeben wurden und Hacker Prämienpunkte gegen Geschenkkarten einlösen konnten.
  - Auch der Automobilzulieferer **Continental** wurde im Sommer 2022 zum Ziel von Cyberkriminellen. Die Untersuchung des Vorfalls hat ergeben, dass die Angreifer trotz etablierter Sicherheitsvorkehrungen auch einen Teilbestand an Daten aus betroffenen IT-Systemen entwenden konnten.
  - Im März 2023 wird von einem Cyber-Angriff auf **Tesla** berichtet, bei sich Hacker aus der Ferne in ein Fahrzeug einwählen und diverse Funktionen ausführen konnten. Dazu zählten u.a. die Betätigung der Hupe, das Öffnen des Kofferraumes, das Einschalten des Abblendlichts sowie die Manipulation des Infotainment-Systems.
  - Software-Schwachstellen in der multimodalen Mobilitäts-App **Moovit (Intel)** führten im August 2023 dazu, dass Sicherheitsforscher zahlreiche Registrierungsdaten (u.a. E-Mail, Kreditkarte) von verschiedenen Benutzerkonten abgreifen und für kostenfreie Fahrten ausnutzen konnten.

Abb. 11: Aktuelle Beispiele von Cyber-Angriffen (2022/23)

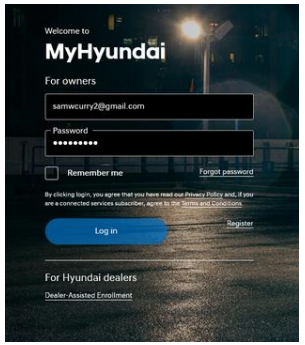


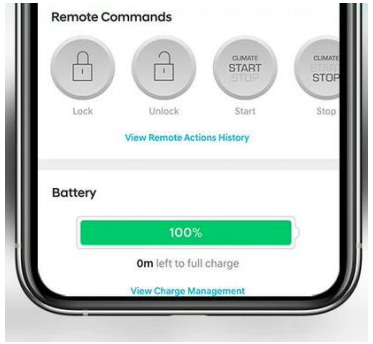
Cyber-Angriffe auf die Automobilindustrie: Internationale Beispiele (2)

Hacker nutzen Schwachstellen, um Zugriff auf **Fahrzeuge, Kundendaten** und **Back-end Infrastrukturen** von Automobilherstellern zu gewinnen. Eine Gruppe „gutartiger Hacker“ um den Sicherheitsforscher Sam Curry hat Ende 2022 nach Schwachstellen in den APIs von Telematik ECUs von Fahrzeugen verschiedener Hersteller gesucht und u.a. folgende aufgedeckt:

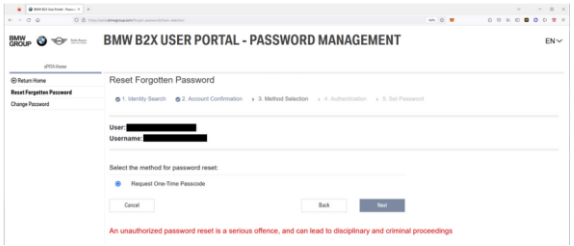
- **Kia, Honda, Infiniti, Nissan, Acura:**
  - Vollständig ferngesteuerte Verriegelung, Entriegelung, Motorstart, Motorstopp, Präzisionsortung, Lichthupe und Hupen von Fahrzeugen nur über die VIN-Nummer
  - Vollständige Fernübernahme von Konten und Offenlegung von personenbezogenen Daten über die VIN-Nummer (Name, Telefonnummer, E-Mail-Adresse, Anschrift)
  - Möglichkeit, Nutzer von der Remote Control ihres Fahrzeugs auszuschließen und den Besitzer zu wechseln
- **Mercedes-Benz:**
  - Zugriff auf Hunderte geschäftskritischer interner Anwendungen über unsachgemäß konfiguriertes SSO, einschließlich...
    - Mehrere Github-Instanzen hinter SSO
    - Unternehmensweites internes Chat-Tool, Möglichkeit zum Beitritt zu fast jedem Kanal
    - SonarQube, Jenkins, verschiedene Build-Server
    - Interne Cloud-Bereitstellungsdienste für die Verwaltung von AWS-Instanzen
    - Interne fahrzeugbezogene APIs
    - Remote Code Execution auf mehreren Systemen
    - Speicherlecks, die zur Offenlegung von personenbezogenen Daten von Mitarbeitern/Kunden führen, Zugriff auf Konten
- **Weitere Automobilhersteller mit Schwachstellen:**

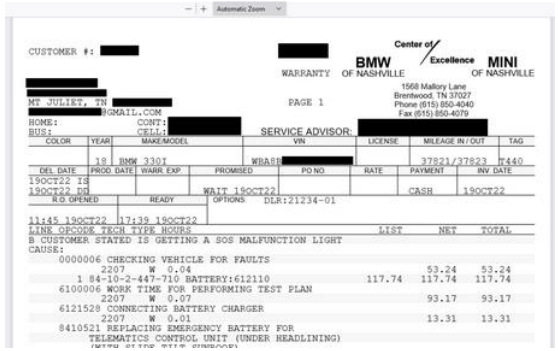
HYUNDAI GENESIS





“If we could do this, it would be full account and **full vehicle takeover** for all remotely enabled Hyundai (and, later we learned, Genesis) vehicles. (…) After putting everything together, we reported the issue to Hyundai and worked with them to confirm the fix.”





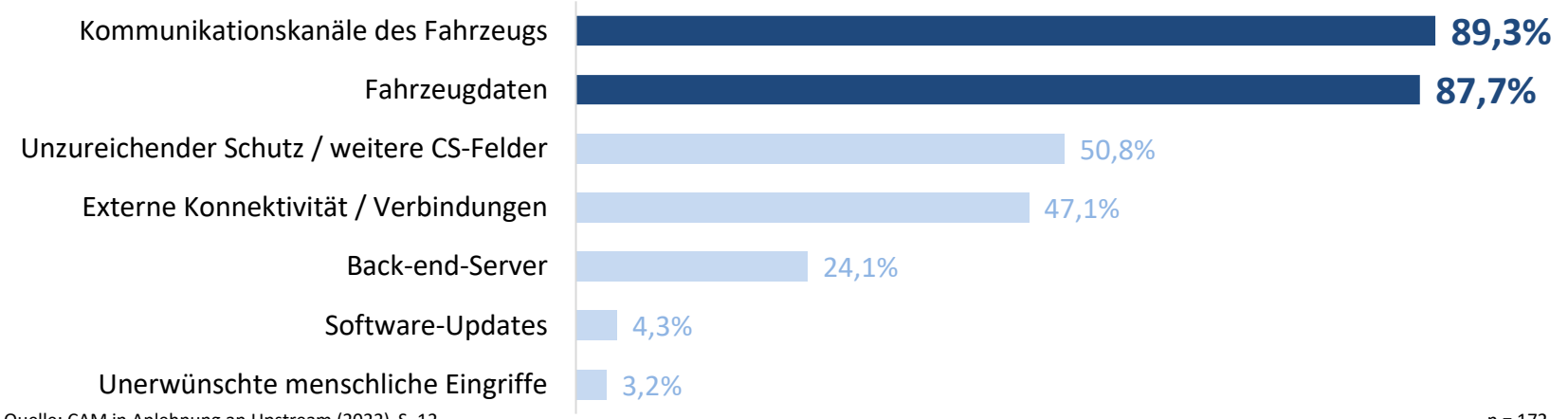
“With our level of access, there was a huge amount of functionality we could’ve performed against BMW and Rolls Royce **customer accounts and customer vehicles**. We stopped testing at this point and reported the vulnerability. The vulnerabilities reported to BMW and Rolls Royce have since been fixed.”

Quelle: CAM in Anlehnung an Curry (2022)

Cyber-Angriffe auf die Automobilindustrie: Kritische Bedrohungsbereiche

- Das Forschungsteam von Upstream analysierte öffentlich gemeldete Cybervorfälle im Automobilbereich, die in den Jahren 2020 und 2021 auftraten, und ordnete sie den sieben Bedrohungskategorien gemäß Anhang 5 der UNECE-R155 zu. Einige Vorfälle fallen in mehr als eine Bedrohungskategorie. Demnach sind die **Kommunikationskanäle (89,3%)** und die **Fahrzeugdaten (87,7%)** am häufigsten von Cyberattacken betroffen.
- Auch in den Medien erfahren Cyberattacken verstärkte Aufmerksamkeit. Einer Studie von VicOne zufolge, die zwischen Anfang 2021 und Juni 2022 Medienberichte zu Sicherheitsthemen in der Automobilindustrie analysierten, hat sich die Bedeutung von **Cyberangriffen** von 9 auf 22% mehr als verdoppelt. Aber auch **schlüssellose Systeme** (25%) und **Ladesäulen** (15%) stehen im Fokus. Anschließende Untersuchungen identifizieren als Conclusio **drei besonders kritische Bereiche**:
  - **Ladestationen für E-Autos**
  - **Cloud APIs**
  - **Schlüssellose Zugangssysteme**

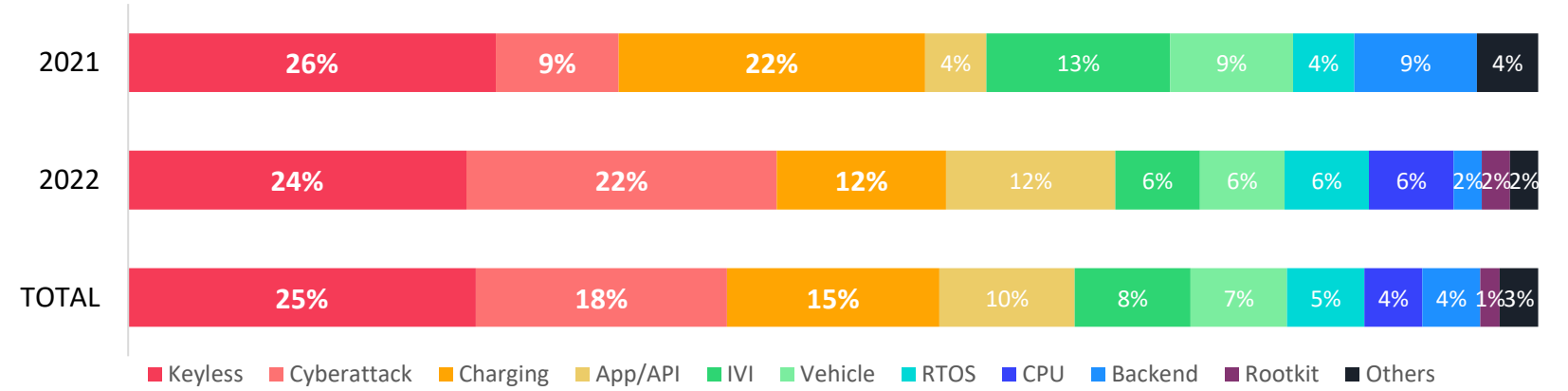
Abb. 12: Häufigkeit von Cyber-Vorfällen nach den Kategorien von WP.29 R155 (2020-2021)



Quelle: CAM in Anlehnung an Upstream (2022), S. 12

n = 172

Abb. 13: Häufigkeit von Sicherheitsthemen in den Automobilnachrichten nach Kategorien (2021-2022)



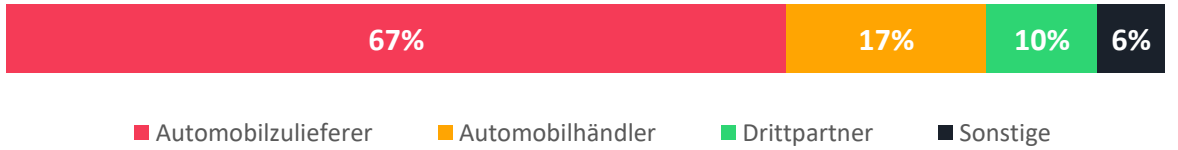
Quelle: CAM in Anlehnung an VicOne (2022), S. 3

n = n/a

Cyber-Angriffe auf die Automobilindustrie: Lieferkette/Zulieferer als Angriffspunkt

- Cyberangriffe in der Automobilindustrie beschränken sich nicht ausschließlich auf große, etablierte Hersteller, sondern treffen verstärkt Zuliefererunternehmen, Automobilhändler und weitere Player entlang der Wertschöpfungskette. Eine Analyse von 52 signifikanten Sicherheitsvorfällen zwischen Januar und Juni 2022 hat ergeben, dass **Automobilzulieferer** zu etwa zwei Dritteln (**67%**) **im Zentrum von Cyberattacken** stehen.
- Die EU-Studie von Enisa (2021), die branchenübergreifend (nicht automotive-spezifisch) Angriffe auf Lieferketten analysierte, wertete von Januar 2020 bis Anfang Juli 2021 24 Angriffe in Europa aus und kam zu folgenden Ergebnissen:
  - 50 % der Angriffe wurden den von der Sicherheitsgemeinschaft bekannten Advanced Persistent Threats (APT)-Gruppen zugeschrieben.
  - 42 % der analysierten Angriffe konnten bisher keiner bestimmten Gruppe zugeordnet werden.
  - 62 % der Angriffe auf Kunden nutzten deren **Vertrauen in ihren Lieferanten** aus.
  - In 62 % der Fälle wurde **Schadsoftware als Angriffstechnik** eingesetzt. Bei der Betrachtung gezielter Vermögenswerte konzentrierten sich die Angreifer bei 66 % der Vorfälle auf den Code der Lieferanten, um gezielte Kunden weiter zu gefährden.
  - Rund 58 % der Supply-Chain-Angriffe zielten auf den **Zugriff von Daten** (überwiegend Kundendaten, darunter personenbezogene Daten und geistiges Eigentum) und rund 16 % auf den Zugriff auf Personen ab.

Abb. 14: Häufigkeit von Cyber-Vorfällen in der Wertschöpfungskette (Jan-Jun 2022)



Quelle: CAM in Anlehnung an VicOne (2022), S. 9

n = 52

Abb. 15: Einteilung von Attacken auf die Lieferkette

Zulieferer		Kunden	
Angriffstechniken zur Beeinträchtigung der Lieferkette	Vermögenswerte der Lieferanten als Ziel des Angriffs auf die Lieferkette	Angriffstechniken zur Beeinträchtigung der Kunden	Vermögenswerte der Kunden als Ziel des Angriffs auf die Lieferkette
• Malware-Infektion • Social Engineering • Brute-Force-Attacke • Ausnutzung von Software-Schwachstellen • Open-Source-Intelligenz (OSINT)	• Vorhandene Software • Software-Bibliotheken • Code • Konfigurationen • Daten • Prozesse • Hardware • Menschen	• Vertrauensvolle Beziehung [T1199 •]Drive-by-Kompromittierung [T1189] • Phishing [T1566] • Malware-Infektion • Physischer Angriff oder Modifikation • Fälschung	• Daten • Persönliche Daten • Geistiges Eigentum • Software • Prozesse • Bandbreite • Finanzen

Quelle: CAM in Anlehnung an Enisa (2021), S. 7

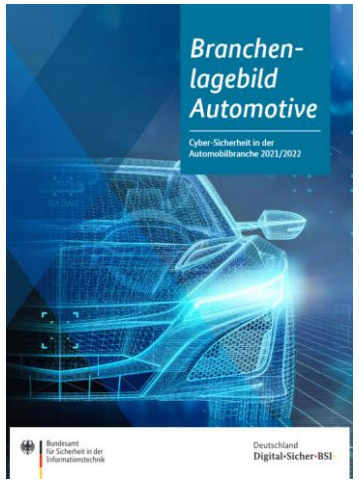
Cyber-Angriffe auf die Automobilindustrie: BSI-Studien 2022/23

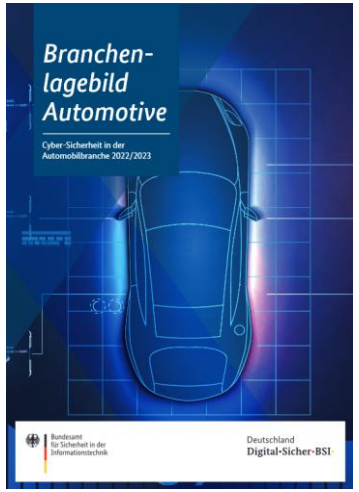
Auch das deutsche Bundesamt für Sicherheit und Informationstechnik (BSI) untersuchte in Studien die Cyberangriffe auf die Automobilbranche, einerseits im Berichtszeitraum Juli 2021 bis Juni 2022 sowie Juli 2022 bis Juni 2023. Im Ergebnis sieht das BSI **Ransomware(-Angriffe)** und **Daten Leaks** weiterhin als die größten operativen Bedrohungen der Cyber-Sicherheit an, insbesondere für die IT-Systeme der Automobilhersteller und deren Zulieferer. Dabei werden folgende Defizite festgehalten:

- Insbesondere bei Ransomware Vorfällen treten **Versäumnisse bei der Prävention** häufig deutlich zu tage. Schlecht gepflegte Systeme, fehlende, veraltete oder nicht überprüfte Software Backups, schwache Administrator Passworte, fehlende Netzsegmentierung u.v.a.m., haben im Fall von Ransomware ein hohes und unmittelbares Schadenpotential.
- Auch das **Verhalten der Mitarbeitenden** spielt eine zentrale Rolle. Einige Angriffe wirken mittlerweile durch Nutzung legitimer Namen und E-Mails so täuschend echt, dass sie nur schwer zu erkennen sind. Hier würde eine bessere Sensibilisierung der Mitarbeitenden helfen.

Darüber hinaus betont das BSI weitere Kernfelder der Cyber Security:

- **Lieferkette**: Bedrohung vor allem durch prorussische Hacktivismus Angriffe. Es kam im Berichtszeitraum zu einigen Vorfällen, die zu Produktionsausfällen oder Störungen bei Zulieferern und IT-Dienstleistern führten. Ein Rüstungs- und Technologiekonzern, der hauptsächlich Kunden aus dem Automotive Sektor beliefert, wurde gleich zweimal Opfer eines Cyber-Angriffs. Dabei kam wiederum Ransomware zum Einsatz.
- **IT-Sicherheitsprobleme von Fahrzeugen bzw. der Straßenverkehrsinfrastruktur:** Die Schließsysteme von Fahrzeugen (die über Funkschlüssel bedient werden) besitzen unzureichende Rollcodes: Einfache Rollcodes reichen für einen wirksamen Schutz nicht aus. Die Schließsysteme (und Wegfahrsperren) müssen mit zusätzlichen kryptographischen Mechanismen gesichert werden.
- **Cyber-Sicherheit beim elektrischen Laden:** Es wird davon ausgegangen, dass sich die Angriffe mit der Wachstumsphase der E-Mobilität stark erhöhen. Angriffsflächen werden beim Ladevorgang etwa in der Phase der Authentifizierung, der Abrechnung oder durch unsichere Updates gesehen (vgl. S. 25 ff.).
- **Verkehrsinfrastruktur:** Einrichtungen wie vernetzte Verkehrssysteme können drahtlos Zustandsinformationen in der Umgebung versenden. Diese sind insbesondere anfällig, da die teils vor vielen Jahren installierten Systeme häufig ohne Cyber-Sicherheitsbetrachtungen vorgenommen wurden.
- **Cyber-Sicherheit in Produktionsanlagen und -prozessen:** Mit der zunehmenden Vernetzung und Automatisierung der Produktion erhöht sich die Angriffsfläche, da diese Systeme auch an das Unternehmensnetzwerk und Dienstleister-Netzwerke angeschlossen sein können. Das BSI betont dabei die Etablierung eines umfassenden Schwachstellenmanagements sowie die cybersicherheitsorientierte Absicherung von Dienstleistern und Fernservices





2. State-of-Practice - Cyber Security in der Automobilindustrie

2.1 Standards und Regulation zum vernetzten Fahrzeugökosystem

2.2 Empirische Erhebungen zu CS-Vorfällen und Angriffen in der Automobilwirtschaft

2.3 Fallstudie/Deep Dive: Cyber Security beim Laden und der Ladeinfrastruktur

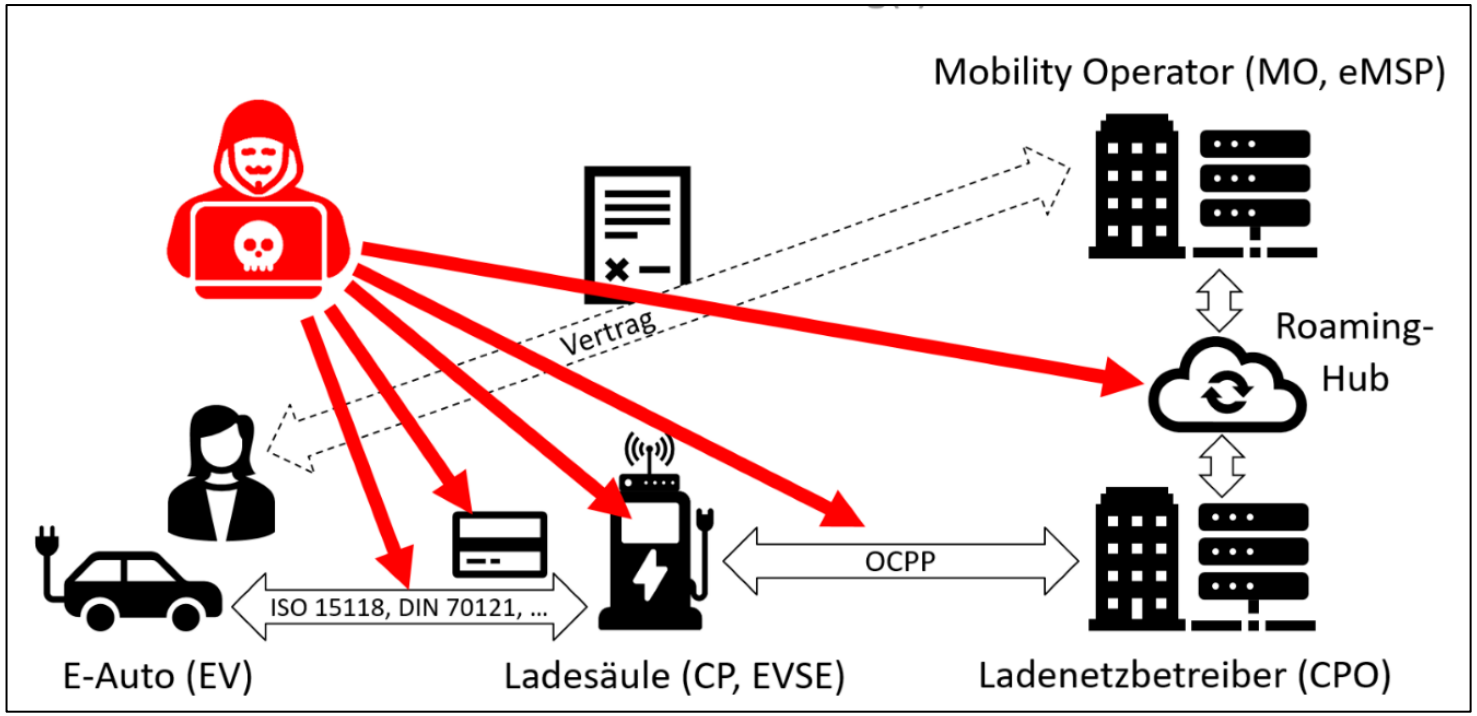
Fallstudie/Deep Dive: Cyber Security beim Laden und der Ladeinfrastruktur*

In verschiedenen Studien (siehe oben) wurde bereits deutlich, dass die Ladeinfrastruktur für Elektrofahrzeugen zu den besonders gefährdeten Cyber-Security Bereichen zählt. Die Ladeinfrastruktur entsteht parallel zur Verbreitung der E-Fahrzeuge unter hohem Druck, um eine große Verbreitung von Ladesäulen zu gewährleisten. Dabei wird die Umsetzung der Cyber Security oft zweitrangig oder überhaupt nicht behandelt. Gleichzeitig ist die Ladeinfrastruktur kein homogenes System, sondern besteht aus Teilen, die von verschiedenen Akteuren und deren Dienstleistern betrieben werden, und die miteinander interoperieren müssen, um Ladevorgänge zu ermöglichen und korrekt abrechnen zu können (siehe Grafik). Durch diese Faktoren ist die Ladeinfrastruktur zu einem leichten Ziel für Angriffe geworden, die nur deswegen noch nicht überhandnehmen, weil das Schadenspotential im Einzelnen sehr überschaubar ist.
Im Folgenden werden Angriffsszenarien für verschiedene Teile der Ladeinfrastruktur aufgezeigt, und der jeweilige Impact beschrieben.

- Die Ladeinfrastruktur kein homogenes System, sondern besteht aus Teilen, die von verschiedenen Akteuren und deren Dienstleistern betrieben werden, und die miteinander interoperieren müssen, um Ladevorgänge zu ermöglichen und korrekt abrechnen zu können

- Das Lade-Ökosystem mit verschiedenen Marktteilnehmern ist komplex und bietet grundsätzlich vielen Angriffspunkte:
  - E-Auto: Netzwerkschnittstelle
  - E-Auto-CP: ISO 15118
  - Ladekarte
  - Ladesäule
  - CP-CPO: OCPP-Verbindung
  - CPO-MSP: OCPI-Verbindung

Abb. 16: Angriffsmöglichkeiten auf das E-Mobility-Ökosystem



Quelle: CAM/rt-solutions.de

* Dieser ‚Deep Dive' zum Thema „Laden/Ladeinfrastruktur" entstand unter Mitarbeit von Ralf Schumann und Georg Lukas von rt-solutions.

Deep Dive: CS beim Laden/Ladeinfrastruktur

Unterscheiden lassen sich Angriffsszenarien

1. für den **Ladevorgang**,
2. die **Ladesäulen**,
3. die **Ladenetz-Backend-Systeme** sowie
4. für **Hub-Anbieter für Roaming.**

1. Angriffe auf den Ladevorgang

Grundsätzlich gibt es beim Ladevorgang zwei Aspekte, die eine Angriffsoberfläche bieten: die Autorisierung (und damit Bezahlung) des Ladevorgangs und die Kommunikation zwischen Fahrzeug und Ladesäule. Die häufigste Form der Autorisierung ist die kontaktlose Ladekarte des eigenen Mobilitätsanbieters (z.B. vom Hersteller des Fahrzeugs oder von einem großen Stromnetzbetreiber). Im Gegensatz zu kontaktlosen Zahlungskarten verfügt sie über keinerlei Schutzmaßnahmen für die Absicherung der Zahlung. Es wird lediglich die Unique ID (UID) der Karte verwendet und dann im Klartext zwischen allen Beteiligten des Ökosystems übertragen. Dass sich solche UIDs trivial kopieren lassen, ist seit 2003 bekannt (Westhues 2003) und wurde auch für E-Ladekarten bereits 2017 demonstriert (Dalheimer, Schwarzladen: Ladekarten manipulieren leicht gemacht, 2017). Erlangt man eine fremde UID, kann man sie mit einem Smartphone auf einen Kartenrohling klonen, oder sogar direkt mit dem Smartphone simulieren, und solange Ladevorgänge auf Kosten des Opfers durchführen, bis der Betrug bei der nächsten Abrechnung auffällt. Dieses System hätte so nicht zum Einsatz kommen dürfen.

Ladevorgänge über die App des Mobilitätsanbieters oder über die Abrechnung mit einem Zahlungsmittel an der Ladesäule haben nicht dieses Problem, sind jedoch weniger komfortabel. Außerdem wurde die verpflichtende Einführung von Zahlungsterminals in neuen Ladesäulen auf Juli 2024 verschoben (Ladesäulenverordnung §8 (4).)

Das neue Plug&Charge-System auf Basis der ISO-15118-Norm verspricht, auf sichere Weise die Anmeldung an der Ladesäule überflüssig zu machen, indem das Auto direkt mit einem kryptografischen Zertifikat des Mobilitätsanbieters ausgestattet wird, und alle Verbindungen verschlüsselt werden. Das System ist hochgradig komplex (und damit anfällig für Fehler und Schwachstellen), da es für jede Rolle eine mehrstufige Public-Key-Infrastruktur (PKI) gibt, und die Provisionierung der Fahrzeuge über verschiedene Wege erlaubt ist (Klapwijk & Driessen-Mutters, 2018). Außerdem ist es in den meisten Bestandsfahrzeugen nicht verfügbar. Mit steigender Verbreitung des Systems ist auch mit der öffentlichen Dokumentation verschiedener Schwachstellen zu rechnen.

Die ISO-15118-Norm beschreibt auch die Datenverbindung zwischen Auto und Ladesäule beim Gleichstrom-Schnellladen (DC). Diese Datenverbindung beruht auf HomePlug AV, einem Verfahren für Datenübertragung über Stromleitungen, gegen das bereits mehrere Angriffe dokumentiert wurden, mit denen sich die Verbindung entschlüsseln und falsche Daten einschleusen lassen (Dudek, 2019), um eine Verbindung zu blockieren (Baker, Köhler, Strohmeier, & Martinovic, 2023) oder sich in eine fremde Plug&Charge-Sitzung einzuhängen (Conti, Donadel, Poovendran, & Turrin, 2022). Mit spezieller Ausrüstung könnte man so einen fremden Ladevorgang unterbrechen, die Ladesäule auf Kosten einer anderen Person nutzen, oder im schlimmsten Fall ein Fahrzeug aus der Nähe beschädigen, indem man falsche Angaben zu Spannung und Stromstärke einschleust.

Pro Vorgang können damit Ladekosten bis zu ca. 60 EUR erschlichen werden, erfordern aber die Anwesenheit des eigenen Fahrzeugs während des ganzen Angriffs an der Ladesäule. Ein großflächiger Angriff auf Fahrzeuge oder das Stromnetz ist damit aber nicht praktikabel, und viele Modelle besitzen Schutz-Sicherungen gegen Überspannung, um physische Schäden zu verhindern.

Deep Dive: CS beim Laden/Ladeinfrastruktur

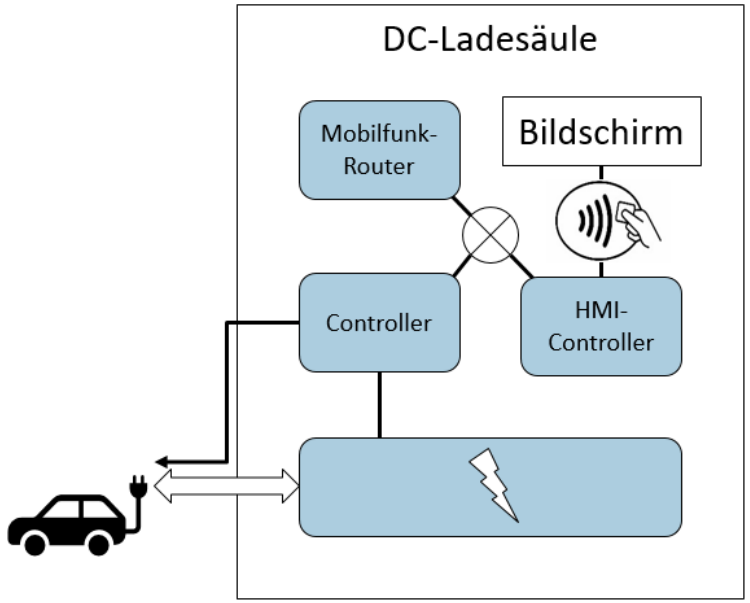
2. Angriffe auf Ladesäulen

Eine Ladesäule hat die Aufgaben, den Nutzer zu identifizieren und zu autorisieren, den Ladevorgang freizuschalten, die übertragene Energie zu messen, und bei DC-Ladesäulen außerdem die Leistung beim Ladevorgang entsprechend der Anforderung des Fahrzeugs zu steuern. Für die Autorisierung und Abrechnung ist eine Datenverbindung mit einem Server des Ladenetzbetreiber notwendig, über die außerdem die Belegung der Ladesäule und andere Live-Daten übertragen werden, und eine Fernwartung über eine Web-Schnittstelle ermöglicht wird. Diese Verbindung wird in den meisten Fällen über Mobilfunk realisiert, und der Zugriff über ein privates APN (Access Point Name) eingeschränkt, das dem Betreiber ein privates Mobilfunk-Datennetz vorgaukelt, in dem sich nur die Ladesäulen und die Backend-Server befinden.
AC-Ladesäulen (Wechselstrom) haben weniger komplexe Anforderungen und kommen oft mit einem einzelnen Controller aus, der alle Aufgaben wahrnimmt.

DC-Ladesäulen haben eine höhere Komplexität und deutlich größere Gehäuse mit einem vollwertigen Bildschirm, und verfügen dafür oft über drei verschiedene Controller – einen für die Ladesteuerung, einen HMI-Controller (Human-Machine Interface) für den Bildschirm, und ein dediziertes Mobilfunk-Modem. Hier werden oft Standardkomponenten aus dem Produktionsbereich mit Embedded Linux eingesetzt, die dank Rapid Prototyping einen schnellen Markteintritt ermöglichen. Zur internen Verbindung der Controller kommt ein handelsübliches Ethernet-Netzwerk zum Einsatz. Der enorme Marktdruck sorgt stellenweise sogar dafür, dass manche Ladesäulen mangels Qualitätssicherung mit einer offenen Hintertür ausgeliefert werden (Johnson, 2023).

Bei der Produktentwicklung wird außerdem oft davon ausgegangen, dass sowohl das interne Netzwerk innerhalb der Ladesäule als auch die Verbindung zum Backend-Server vertrauenswürdig sind, von dort also keine Angriffe kommen können. In der Praxis sind lediglich leicht erhältliche Werkzeuge und etwas Übung notwendig, um das Schloss an einer schlecht bewachten Ladesäule gewaltfrei zu öffnen, und Zugriff auf die internen Systeme zu erhalten. So erhält man Zugriff auf die interne Kommunikation und meist schlecht gesicherte Wartungsschnittstellen, über die sich Kunden-UIDs auslesen lassen oder eine manipulierte Firmware aufgespielt werden kann (Dalheimer, Schwarzladen III: Mit USB zum Profit, 2017). Eine solche Manipulation ist nur schwer aufzudecken, und kann als dauerhafte „Wanze“ verwendet werden, um weitere Kundendaten auszulesen, den Controller der Ladesäule (zeitverzögert) lahmzulegen, oder um das Backend-Netzwerk und andere Ladesäulen anzugreifen. Die gleiche Art von Angriff kann auch mithilfe der in der Ladesäule eingebauten SIM-Karte durchgeführt werden, die auf das APN-Netz des Ladenetz-Betreibers zugreifen kann.

Abb. 17: Typischer Aufbau einer Ladesäule



Quelle: CAM/rt-solutions

Deep Dive: CS beim Laden/Ladeinfrastruktur

3. Angriffe auf Ladenetz-Backend-Systeme

Während die Backend-Server oft nicht direkt aus dem Internet erreichbar sind, oder über entsprechende Härtung verfügen, wird nicht mit einem Angriff durch eine Ladesäule gerechnet. So gelang es dem Autor im Sommer 2022 während der Sicherheitsanalyse einer Ladesäule, durch einen trivialen Angriff auch ausführbaren Code in das Backend-System des Betreibers einzuschleusen, mit dem es auch möglich wäre, die Kontrolle über das Backend-System und alle daran angebundenen Ladesäulen zu erhalten. Die Schwachstelle wurde unmittelbar an die Entwickler gemeldet, aber nach einem Jahr immer noch nicht vollständig beseitigt.

Im schlimmsten Fall kann auf diesem Weg das gesamte Ladenetz eines Betreibers oder eines Verbunds auf einen Schlag derart sabotiert werden, dass die Controller komplett ersetzt werden müssen, ähnlich wie das 2022 beim Angriff auf das KA-Sat-System gelang (Ermert, 2022).

Oft ist dafür nicht einmal die Ausnutzung von Schwachstellen notwendig, weil die Ladesäulen von einigen Integratoren mit den (öffentlich dokumentierten) Standard-Passwörtern der Hersteller betrieben werden, um die Störungsbeseitigung zu erleichtern.

3. Hub-Angriffe

Die schnell wachsende Anzahl von Ladenetzbetreibern (Charge Point Operators, CPO) und Mobilitätsanbietern (Mobility Operators, MO) machte es notwendig, zentrale Strukturen zur Vermittlung von Ladevorgängen zu etablieren, damit nicht jeder Betreiber mit jedem anderen ein direktes Vertrags- und Kommunikationsverhältnis braucht. Roaming-Hubs übernehmen diese Aufgabe, indem sie Ladeanfragen an alle teilnehmenden Partner weiterleiten, so dass der passende Mobility Operator den Ladevorgang autorisieren kann. Am Ende des Ladevorgangs wird ein Charge Detail Record (CDR) mit Informationen über die genutzte Ladesäule, die Ladezeit, den entstandenen Kosten und der Vertragsnummer über den Hub übermittelt.

In Europa sind nur einige wenige Hub-Anbieter tätig. Schließt man sich als vorgetäuschter Mobility Operator einem Hub an, kann man in Echtzeit alle Ladeanfragen mit dem Standort der jeweiligen Ladestation und der UID der Kundenkarte verfolgen, die über den Hub geschickt werden, und so ungefähre Bewegungsprofile von E-Fahrzeugen erstellen. Der Hub-Betreiber bekommt dabei auch die folgende Kommunikation zwischen CPO und MO mit, und die Vertragsnummer des jeweiligen Nutzers, so dass auch Zahlungsvorgänge von verschiedenen Ladesäulen desselben Anbieters und die zugeordnete Vertragsnummer nachverfolgbar werden. Damit werden E-Mobility-Hubs auch zu besonders attraktiven Angriffszielen für fremde staatliche Akteure.

Deep Dive: Laden/Ladeinfrastruktur

Cybersecurity Report 2022 von VicOne (2022)

VicOne nennt in seinem Report drei zentrale Angriffpunkte im Bereich der **Ladeinfrastruktur** (2022, S. 13):

"1. CAN bus-based communication protocol between an EV and a charging station
CAN bus-based protocols are often used on EV and charging station communications, and always transfer data by plain text. This gives hackers opportunities to hijack the sessions to deploy MitM attacks. They could also transfer malicious code to the EV or charging station.

2. App/Cloud services for EV charging stations
EV charging stations are usually connected to the cloud for transactions and billing procedures. Some EVs even have apps to give users a more convenient experience. In the context of cybersecurity, this is a traditional attack surface. An attacker could gain privileges to gather user information from mobile devices or penetrate the cloud server.

3. Radio communications
Radio communications, RFID, Bluetooth, and customized radio signals are frequently used on EV charging systems. These could become remote attack surfaces that attackers use to access the EV components. For example, hackers could remotely open the charging port or transfer malicious code to the EV or charging station to gain control."

Quelle: VicOne 2022, S. 13 (https://vicone.com/files/rpt-automotive-cybersecurity-in-2022.pdf)

Unterbrechung von Schnellladevorgängen bei CCS (2022)

Auch im Zuge des Hochlaufs der Elektromobilität werden zunehmend Schwachstellen erkannt. Im Rahmen einer Forschungsarbeit (9) wurde eine Schwachstelle im Combined Charging System (CCS), einem weit verbreiteten Ladestandard für batterieelektrische Fahrzeuge, entdeckt. Ziel des Angriffs ist die Unterbrechung eines Ladevorganges von einem oder mehreren Elektrofahrzeugen. Es handelt sich um einen Angriff auf die im CCS verwendete Kommunikationstechnologie Power Line Communication (PLC). Der CCS-Standard wird in Ladesystemen für eine Vielzahl von Transportsystemen (LKW, Busse, Fähren, Flugzeuge, etc.) angewendet sowie perspektivisch auch in Netzanwendungen. Die Schwachstelle ist nur für das Schnellladen (DC Charging) relevant. Da die ausgetauschten Informationen sicherheits- und steuerungsrelevant sind, wird bei einer Störung der Kommunikation der Ladevorgang abgebrochen. Dieses Verhalten ist von den einschlägigen Standards vorgegeben. Dies wird bei dem Angriff ausgenutzt und die Steuerkommunikation zwischen Elektrofahrzeug und Ladegerät durch Funksignale derart gestört, dass es zu einem Verbindungsabbruch zwischen Ladesäule und dem aufzuladenden Elektrofahrzeug kommt. Für einen vollständigen Paketverlust der PLC-Kommunikation reiche laut Autoren eine Sendeleistung von 10mW, um 10 Meter Abstand (in einer Laborumgebung) zu überwinden, bei höheren Sendeleistungen können bis zu 47 Meter erreicht werden. Die Auswirkungen eines Angriffs bleiben glücklicherweise überschaubar, da hierbei kein bleibender Schaden am Fahrzeug oder Ladegerät entsteht. Durch das beschriebene Szenario könnte aber die Verfügbarkeit des Ladens bei öffentlich zugänglichen Schnelladesäulen lokal eingeschränkt werden.
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Brancheneinlagebild/branchenlagebild-automotive-2021_2022.pdf?__blob=publicationFile&v=8

S. Köhler, R. Baker, M. Strohmeier, I. Martinovic: „Brokenwire: Wireless Disruption of CCS Electric Vehicle Charging", arXiv preprint, Februar 2022, https://arxiv.org/abs/2202.02104

Deep Dive: CS beim Laden/Ladeinfrastruktur

Zusammenfassung

- Während lokale Angriffe auf Ladevorgänge nur ein kleines Schadensausmaß haben, bei dem man auf fremde Kosten laden oder einen fremden Ladevorgang unterbrechen kann, um früher an die Reihe zu kommen, erhalten Angreifer, die in das Innere einer Ladesäule vordringen, leicht Zugriff auf Zahlungsdaten vieler verschiedener Nutzer, und können die Ladesäule auch als Sprungpunkt für Angriffe auf das Backend-Netzwerk des Netzbetreibers nutzen. Diese Netze sind oft unzureichend gehärtet, so dass die Angreifer dort unerkannt die Kontrolle über Backend-Server und weitere Ladestationen übernehmen können, oder im schlimmsten Fall auf die Lastregelung des regionalen Stromnetzes Einfluss nehmen könnten.
- Greift man die Hub-Infrastruktur an, die zwischen Ladenetzbetreibern und Mobilitätsanbietern vermittelt, so kann man anhand der vermittelten Ladevorgänge Bewegungsprofile von Fahrzeugen machen, und mit den personenbezogenen Daten der jeweiligen Vertragsinhaber verknüpfen.
- Um die Kompromittierung von Ladesäulen, Backend-Services und der Hub-Infrastruktur zu verhindern, müssen alle Betreiber, die aus dem IT-Betrieb bekannten und für KRITIS-Anbieter geforderten technischen und organisatorischen Maßnahmen umsetzen, um die Systeme zu härten, laufende Angriffe zu erkennen, unterbrechen und analysieren zu können.

Tab. 2: Übersicht der Angriffsszenarien

Ziel	Angriff	Schadenspotential	Gegenmaßnahmen
Ladevorgang	**UID-Cloning**	Laden auf fremde Kosten	Regelmäßige Prüfung der Abrechnungen
Ladevorgang	**ISO15118-Angriffe**	Abbruch eines Ladevorgangs, Laden auf fremde Kosten, ggfs. Fahrzeug-Sabotage	Nachträgliche Sicherung der Protokolle nicht realistisch; Schutz der Fahrzeuge durch Sicherungen
Ladesäule	**Physischer Zugriff auf Daten**	Laden auf Kosten vieler verschiedener Nutzer	Einbruchserkennung, Absicherung und Verschlüsselung der internen Datenschnittstellen, Pen-Testing der Ladesäulen, Härtung durch Integratoren
Ladesäule	**Firmware-Manipulation**	Sabotage der Ladesäule, Angriffe auf das Backend, „Kostenlose“ Ladevorgänge	
Backend	**Privilege Escalation**	Übernahme der Fernwartung aller Säulen im Verbund, Einspielen von Selbstzerstörungs-Firmware	Absicherung und Verschlüsselung der Kommunikation mit Ladesäulen, Pen-Testing der Schnittstellen und Server
Hub	**MO vortäuschen**	Zugriff auf partielle Bewegungsprofile	Mittelfristig nicht abwendbar, langfristig Neuentwicklung von datenschutzkonformen Protokollen für Hub-Kommunikation
Hub	**Datenabgriff**	Zugriff auf umfangreiche Bewegungsprofile	Durchgehende Verschlüsselung der Kommunikation, Härtung und Pen-Testing der Server, langfristig Neuentwicklung von datenschutzkonformen Protokollen für Hub-Kommunikation

Quelle: CAM/rt-solutions

2. State-of-Practice - Cyber Security in der Automobilindustrie

2.1 Standards und Regulation zum vernetzten Fahrzeugökosystem

2.2 Empirische Erhebungen zu CS-Vorfällen und Angriffen in der Automobilwirtschaft

2.3 Fallstudie/Deep Dive: Cyber Security beim Laden und der Ladeinfrastruktur

2.4 Zusammenfassende Thesen und Schlussfolgerungen

State-of-Practice der Cyber Security: Zusammenfassende Thesen und Schlussfolgerungen (1)

- Folgende **relevante Herausforderungen** ergeben sich bei Cyber Security in der Automobilbranche:
  - Hoher **Wettbewerbs- und Time-to-Market-Druck** durch die Kundenwünsche nach Connected Cars / Connected Services, bei denen **Cyber Security Aspekte in den Hintergrund** gedrängt werden können. CS-Vorfälle können dann zu einem großen Imageschaden führen.
  - Die Automotive Cyber Security umfasst grundsätzlich den gesamten **Produktlebenszyklus des Fahrzeugs** von der Entwicklung, über die Produktion bis hin zur Fahrzeugnutzung. Der lange Produktlebenszyklus und die hohe **Variantenvielfalt** erschweren die Gewährleistung von Cyber Security deutlich. Die verschiedenen Phasen des Produktlebenszyklus‘ bergen dabei **unterschiedliche Angriffspunkte und Risiken**.
  - Cyber Security Aktivitäten beschränkten sich in der Vergangenheit vornehmlich auf Absicherung von Schwachstellen zum Zeitpunkt der Fahrzeugproduktion. Zukünftig müssen Hersteller und ihre Lieferanten Strukturen etablieren, die von Beginn der Produktentwicklung an auf eine kontinuierliche Absicherung des gesamten Produktlebenszyklus ausgerichtet sind. Die **verteilte Verantwortung bei der komplexen Wertschöpfungskette** im großen Lieferanten- und Partnernetzwerk erhöht die Anfälligkeit für Cyberangriffe.
- Die regulativen Vorgaben zur Cyber-Sicherheit in Kraftfahrzeugen (gemäß der UNECE Regelung UN R155 (15) / Verordnung (EU) 2018/858)) müssen seit Juli 2022 von den Herstellern verpflichtend für alle neuen Fahrzeugtypen umgesetzt werden. Ab **Juli 2024** unterliegen auch alle **neuen oder bestehenden Fahrzeugtypen** der UN R155-Typgenehmigung für Cybersicherheit. Die Umsetzung der verschiedenen Standards ist eine hohe Herausforderung für die Branche.
- **Eine Meta-Analyse** zu den Cyber-Angriffen auf Fahrzeuge und Unternehmen der Automobilwirtschaft zeigt die **Dringlichkeit und wachsende Bedeutung** des Themas. Gleichzeitig offenbaren die Auswertungen auch die **bisherigen Angriffspunkte** auf die Cybersicherheit der internationalen Automobilwirtschaft. Die Ergebnisse können wie folgt zusammengefasst werden:
  - Die **Quantität und Qualität der Angriffe stieg** in den letzten Jahren erheblich: Die Automobilindustrie im Allgemeinen und die Zulieferunternehmen im Besonderen sind immer häufiger von Cybervorfällen betroffen.
  - “**Ransomware Angriffe“** gelten derzeit als die größte operative Bedrohung der Cyber-Sicherheit, insbesondere für die IT-Systeme der Automobilhersteller und deren Zulieferer. Dabei spielen **Versäumnisse bei der Prävention** als auch beim **Verhalten der Mitarbeitenden** eine zentrale Rolle.

State-of-Practice der Cyber Security: Zusammenfassung und Schlussfolgerungen (2)

- Die **Lieferkette bzw. die komplexe Zuliefererlandschaft** gelten als große Schwachstelle und stellen zentrale Angriffspunkte mit einer hohen Eintrittswahrscheinlichkeit und einem hohem Schadensausmaß dar. Cyber Security befindet sich bei vielen Zulieferer und Dienstleistern noch auf einem niedrigen Niveau. Mit der zunehmenden Vernetzung und Automatisierung erhöht sich zusätzlich die Angriffsfläche, da diese Systeme auch an das Unternehmensnetzwerk und Dienstleister-Netzwerke angeschlossen sein können.
- Die **Ladeinfrastruktur für Elektrofahrzeugen** wird verschiedenen Studien zufolge zu den besonders gefährdeten Cyber Security Bereichen zählt. Beim Aufbau der Ladeinfrastruktur besteht - parallel zur Verbreitung der E-Fahrzeuge – ein hoher Umsetzungsdruck. Die Ladeinfrastruktur ist dabei kein homogenes System, sondern besteht aus Teilen, die von verschiedenen Akteuren und deren Dienstleistern betrieben werden, und die miteinander interoperieren müssen, um Ladevorgänge zu ermöglichen und korrekt abrechnen zu können. Das Lade-Ökosystem mit verschiedenen Marktteilnehmern ist dadurch sehr komplex und bietet grundsätzlich vielen Angriffspunkte. Angriffsszenarien ergeben sich für den **Ladevorgang**, die **Ladesäulen**, die **Ladenetz-Backend-Systeme** sowie für **Hub-Anbieter für Roaming.**
- Eine transparente Berichterstattung von Automobilunternehmen zu Cyberangriffen ist noch deutlich unterentwickelt. Grundsätzlich würde eine transparente Berichterstattung zu Cyberangriffen und deren Bewältigung das **Bewusstsein in der Branche** für die Gefahren und Risiken erhöhen und könnte andere Unternehmen dazu motivieren Programme und Maßnahmen für einen möglichst umfassenden Schutz von Cyber Security zu treffen. Im Rahmen der Studie ist die transparente Kommunikation zu Cyberangriffen auch ein **Indikator für eine professionelle Cyber Security Kultur** in den Unternehmen. Es wird durch die Berichterstattung anerkannt, dass Cyber-Angriffe zum unternehmerischen Alltag gehören und sie durch eine hohe Qualität des Cyber Security Managementsystems bewältigt werden müssen.

3. Bewertung der Qualität von Cyber Security in Automobilunternehmen

3.1 Heuristisches Modell der Bewertung von Cyber Security Performance

Heuristisches Modell der Bewertung von „Cyber Security Performance“ in der Automobilindustrie

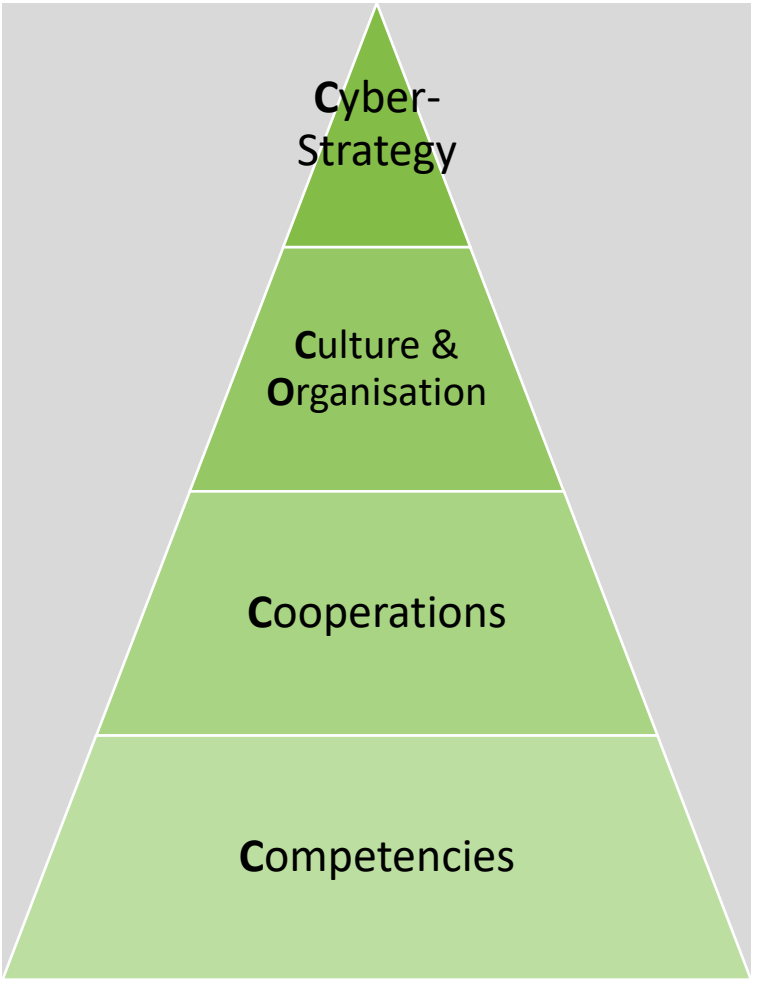
Die Cyber Security von Unternehmen der Automobilindustrie gewinnt im Zuge der Vernetzung des Kernprodukts Fahrzeug sowie der Digitalisierung der Unternehmen und der gesamten Wertschöpfungskette stark an Bedeutung. Die Unternehmen unterscheiden sich jedoch bzgl. der Qualität der Konzeption und Umsetzung von Cyber Security erheblich. Eine hohe Cyber Security Performance im Unternehmen erhöht nicht nur die Resilienz vor den zunehmenden Cyber-Angriffen und ermöglicht eine schnelle Erkennung und angemessene Reaktion auf entsprechende Vorfälle. Vielmehr können dadurch die Chancen von Digitalisierung und Vernetzung in den eigenen Produkten sowie in den Wertschöpfungsstufen der Entwicklung und Produktion besser genutzt werden.

Auf Basis von Experteninterviews (vgl. Anhang) und einer Analyse von Sekundärquellen wurde ein heuristisches **Modell zur empirischen Bewertung der Cyber Security Performance** von Automobilunternehmen entwickelt. Dabei wird davon ausgegangen, dass für eine hohe Qualität von Cyber Security im Unternehmen breite **Kompetenzen** erforderlich sind, die nicht auf einzelne Abteilungen (z.B. IT-Abteilung) beschränkt sein dürfen und über gesetzliche Anforderungen (Compliance) hinausgehen müssen. Dabei sollten Cyber Security Kenntnisse in der gesamten **Organisation** sowie bei verbundenen **Kooperationspartnern** der Wertschöpfungskette verankert werden. Entsprechend muss sich Cyber Security auch in der **Kultur** der Unternehmen widerspiegeln, um das Verhalten der Mitarbeiter im Hinblick auf Cybersicherheit nachhaltig positiv zu beeinflussen. Der kulturelle Wertekanon findet seinen Wiederklang in einer entsprechenden **Cyber-Strategie**, also in den Zielen der Unternehmenspolitik sowie im Leadership.

Das „4C“-Modell vereinigt vor diesem Hintergrund relevante Leistungskriterien von Cyber Security in vier Dimensionen: Kompetenzen (**C**ompetencies), Kooperationen (**C**ooperations), Kultur & Organisation (**C**ulture & Organisation) sowie die Cyber-Strategie (**C**yber Strategy).

Die einzelnen Dimensionen und Leistungskriterien werden nachfolgend vorgestellt und empirisch fruchtbar gemacht.

Abb. 18: Heuristisches Modell zur empirischen Bewertung von Cyber Security Performance in der Automobilindustrie



Quelle: CAM

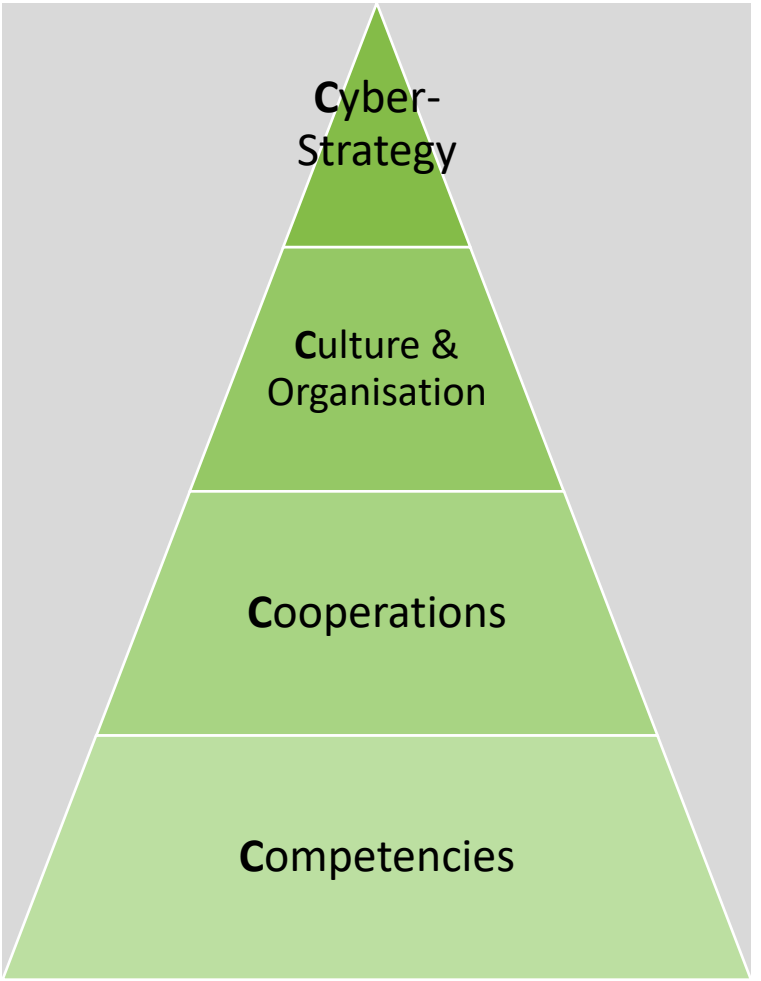
„4C“-Modell: *Competencies, Cooperations, Culture & Organisation, Cyber Strategy*

Die vier Dimensionen **Co**mpetencies, **Co**operations, **C**ulture & **O**rganisation und **C**yber **S**trategy des „4C“-Modells zur Messung der Cyber Security Performance werden wie folgt definiert:

- **C**ompetencies: Unter Cyber Security Kompetenzen wird das Know-how im Unternehmen bzw. die Kenntnisse bzw. Fähigkeiten und Fertigkeiten des Unternehmens und der Mitarbeiterschaft bezogen auf die Cybersicherheit verstanden.
- **C**ooperations: Unter Kooperationen wird die Cyber Security Qualität der Kooperationspartner/ des Lieferantennetzwerks bzw. der gesamten Wertschöpfungskette betrachtet.
- **C**ulture & Organisation: Die Cyber-Kultur umfasst den **Wertekanon** eines Unternehmens bezüglich Cyber Security. Entsprechende Ausprägungen beeinflussen das Erkennen von Cybersicherheits-probleme durch Mitarbeiter sowie die Offenheit der Kommunikation und das Einbringen von Verbesserungen. Sie hängt eng mit der Vorbildfunktion der Führung des Unternehmens für Cyber Security zusammen. Die Cyber-Kultur manifestiert sich auch in einer entsprechenden **Qualität der Organisation und Prozesse** von Cyber Security, in denen Verantwortlichkeiten und Pflichten bekannt sind und alle Geschäftseinheiten in Cyber-Initiativen eingebunden sind. Dabei geht es auch um die Quantität/Qualität von Ressourcen und Ausstattung der Belegschaft in allen Geschäftsbereichen, um Cyberangriffe abzuwehren und Sicherheitsmaßnahmen umzusetzen.
- **C**yber Strategy: Die strategische Dimension dreht sich um die Existenz und Qualität von hochrangigen Handlungsprogrammen und Richtlinien der Cyber Security im Unternehmen. Dabei sind auch der Grad der Integration von Cyber Security in das Risikomanagement, die Prozesse zur Erkennung von und die Reaktion auf Angriffe, die Qualität des Reportings an den Vorstand sowie unabhängige Cyber-Sicherheitsrisikobewertungen relevant (z.B. Überprüfung der Cyber Security durch „friendly hackers“).

Für die verschiedenen Dimensionen des „4C“-Modells werden zur Operationalisierung des Cyber Security Messkonzepts nachfolgend **Kriterien** zur Messung entwickelt.

Abb. 18: Heuristisches Modell zur empirischen Bewertung von Cyber Security Performance in der Automobilindustrie



Quelle: CAM

3. Bewertung der Qualität von Cyber Security in Automobilunternehmen

3.1 Heuristisches Modell der Bewertung von Cyber Security Performance

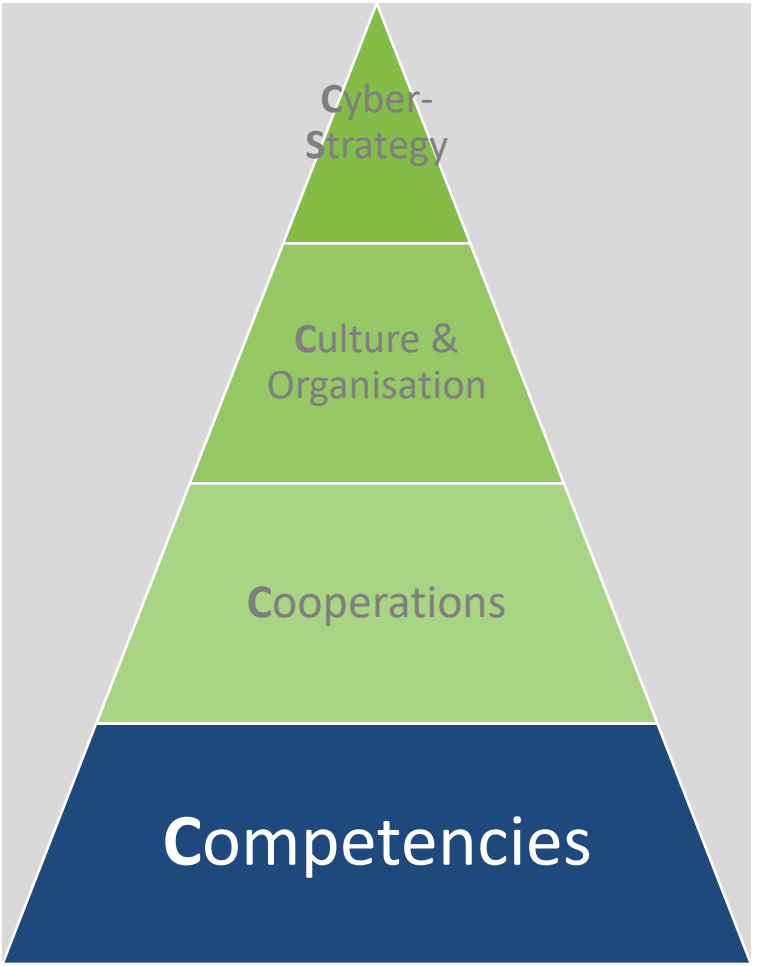
3.2 Kriterien und Indikatoren zur Messung

„4C“-Modell: Kriterien zur „Messung“ der Qualität der CS-Kompetenzen

Zur empirischen Bestimmung der **Leistungsqualität** der Cyber Security in den Automobilunternehmen werden auf Basis des „4C“-Modells operationalisierbare **Kriterien und Indikatoren** für die einzelnen Bewertungsbausteine in Form eines systematisierten Fragenkatalogs vorgestellt.

Bewertungskriterien	*Beispielhafte Fragestellungen/Indikatoren*
Kompetenz- und Schwachstellenanalyse	Gibt es einen speziellen Report zum Status der CS-Kompetenzen im Team, inkl. der Defizite sowie einen Plan, um die Defizite zu adressieren? Sind auf der Vorstandsebene die wichtigsten Bedrohungen bekannt und die Programme zur Bewältigung von Angriffen? Wie schneiden die Mitarbeiter bei Sensibilisierungsschulungen grundsätzlich ab?
Cyber Awareness	Wird die Belegschaft umfassend zum Thema Cyber Security sensibilisiert? Gibt es eine gute Mitarbeiterbindung in Schlüsselpositionen im Bereich Cybersicherheit? Wie hoch ist der Beteiligungsgrad bei Phishing-E-Mails? Bis zu welchem Grad werden Vorfälle durch Mitarbeiter gemeldet?
Fort-/Weiterbildung	Wie oft werden Schulungen und Workshops zu aktuellen bzw. zukünftigen Normen und Sicherheitsstandards verpflichtend angeboten? Werden diese auch bereichsübergreifend angeboten?

Abb. 19: Heuristisches „4C“- Bewertungsmodell

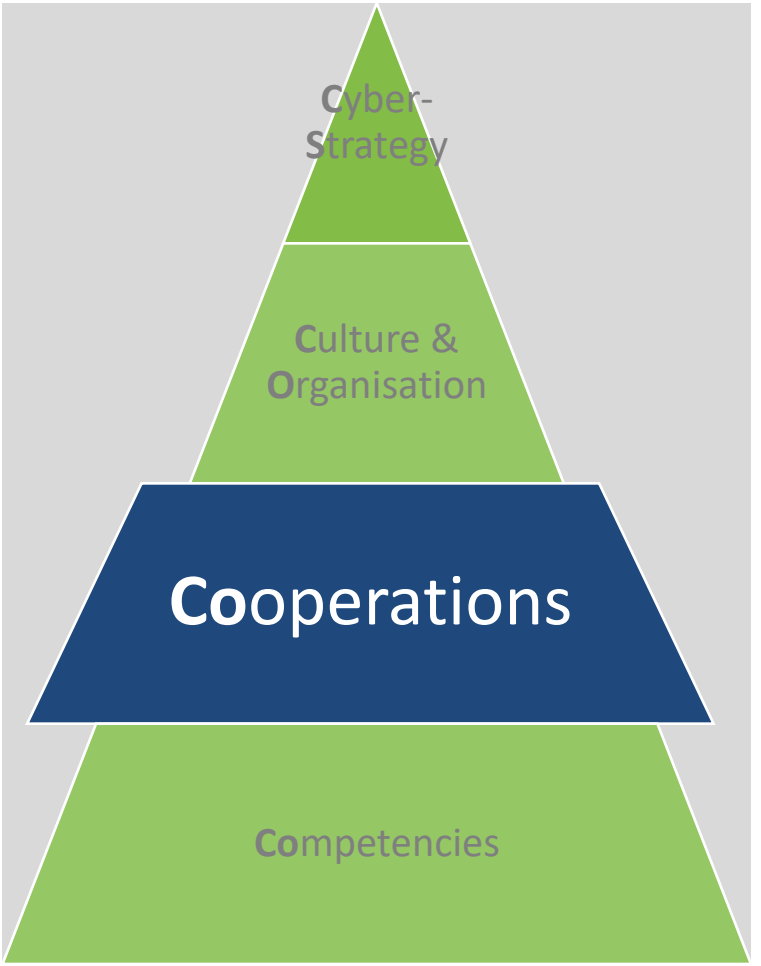


Quelle: CAM

„4C“-Modell: Kriterien zur „Messung“ der Qualität der CS-Kooperationen

Bewertungskriterien	*Beispielhafte Fragestellungen/Indikatoren*
Supplier Performance	Wird die Leistung der Lieferanten regelmäßig anhand definierter Kennzahlen gemessen (z.B. Prozentsatz der Lieferanten/Subunternehmer, die bewertet wurden, wann sie zuletzt bewertet wurden)? Ist dies für die Vorstandsmitglieder einsehbar?
Einbindung der Zulieferer	Wird das Zulieferer-/Wertschöpfungsnetzwerk in die Bedrohungsbewertung des Unternehmens integriert? Finden regelmäßig Übungen zum Umgang mit CS-Vorfällen im Lieferanten-/Wertschöpfungsnetzwerk statt?
Tracking von CS-Bedrohungen in der Lieferkette	Werden CS-Vorfälle, die sich ggfs. nicht auf das eigene Unternehmen auswirken, regelmäßig überwacht und analysiert? Erhält der Vorstand eine kontinuierliche Berichterstattung der größten CS-Bedrohungen im Lieferanten-/Wertschöpfungs-netzwerk?

Abb. 19: Heuristisches „4C“- Bewertungsmodell

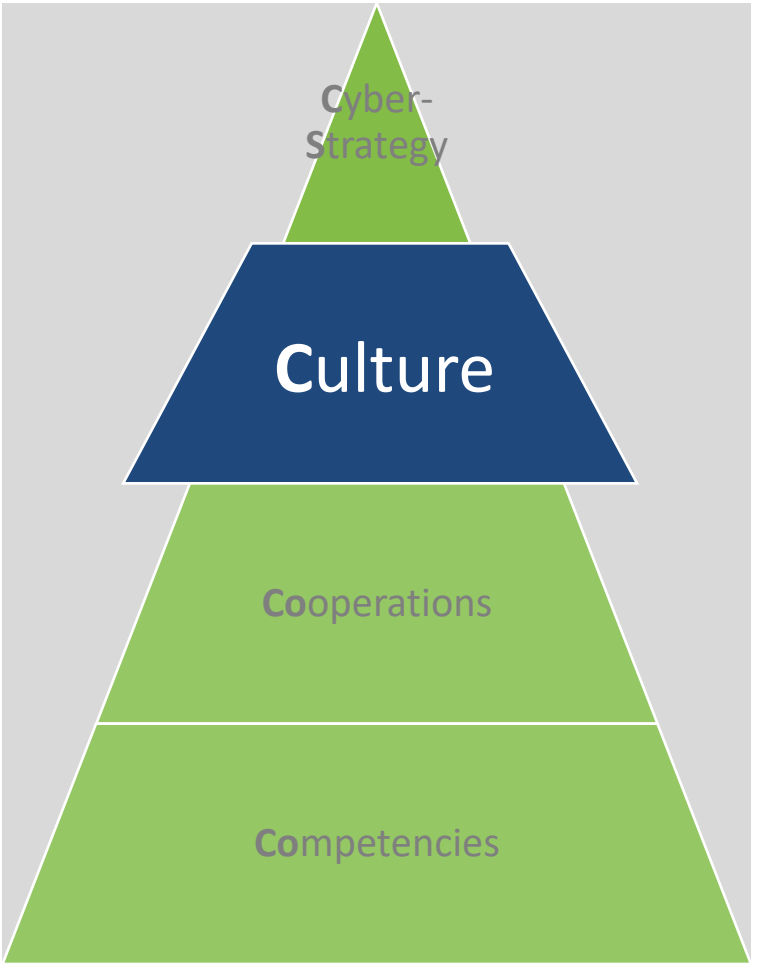


Quelle: CAM

„4C“-Modell: Kriterien zur „Messung“ der Qualität der CS-Kultur

Bewertungskriterien	*Beispielhafte Fragestellungen/Indikatoren*
Leadership	Weiß das Management, was zu tun ist, wenn ein (möglicher) Angriff stattfindet? Spricht der Vorstand mit Mitarbeitern offen und positiv darüber, warum Cybersicherheit für das Unternehmen wichtig ist?
Kommunikation (intern)	Besteht ein kollaborativen Ansatz der Gestaltung von Sicherheitsrichtlinien und Prozessen? Gibt es eine hohe Transparenz bei der Kommunikation zu Cyberangriffen?
Reporting und Lernen	Werden Vorfallsberichte genutzt, um über Ursachen, Reaktionsmuster (inkl. Geschwindigkeit) und Verbesserungen der CS-Organisation nachzudenken? Wie können CS-Kennzahlen im Hinblick auf Erfolge formuliert werden (statt: Wie viele Personen haben auf eine Phishing-Mail geklickt, eher: Wie viele haben die Phishing-Mail gemeldet)
Transparenz der Kommunikation (extern)	Erfolgt nach einem registrierten Angriff unverzüglich eine externe Berichterstattung? In welchem Detailgrad werden die Informationen zum CS-Angriff aufbereitet (z.B. Angriffspunkte, Schadensausmaß etc.)? Existieren dokumentierte „lessons learnt“ zur zukünftigen Risikoreduzierung (z.B. Welche Schwächen haben den Angriff begünstigt?)?

Abb. 19: Heuristisches „4C“- Bewertungsmodell

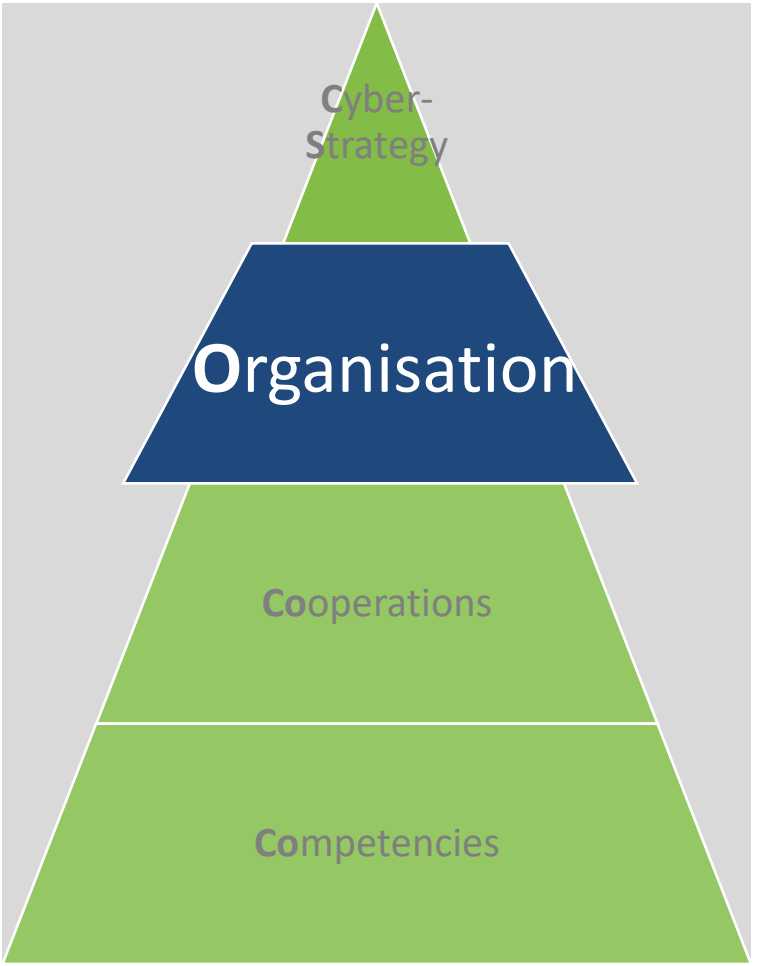


Quelle: CAM

„4C“-Modell: Kriterien zur „Messung“ der Qualität der CS-Organisation

Bewertungskriterien	*Beispielhafte Fragestellungen/Indikatoren*
Umsetzungsgrad und Ausstattung	Werden alle geltenden Standards und Regularien (über-)erfüllt? Besteht ein funktionierendes Cyber Security Management System (CSMS)? Sind die der Belegschaft zur Verfügung gestellten Ressourcen/Ausstattungen sowohl quantitativ als auch qualitativ ausreichend, um Cyberangriffe abzuwehren und Sicherheitsmaßnahmen umzusetzen?
Priorisierung	Arbeiten alle Geschäftseinheiten (HR, Recht, PR) gemeinsam an CS-Initiativen? Sind außerhalb der IT weitere Geschäftsbereiche mit der Erarbeitung, Kontrolle und Verbesserung des Cybersicherheitskonzepts betraut?
Verantwortlichkeit/ Rechenschaft	Existieren klare Definitionen von Verantwortlichkeit und Rechenschaftspflichten bei der Berichterstattung/Kommunikation von Cybersicherheit?
Wirksamkeit	Inwiefern vereinfachen Key Performance Indicator (KPI)-Dashboards den Berichtsprozess und versorgen den Vorstand mit klaren sowie aktuellen Informationen, um eine gute Entscheidungsfindung zu unterstützen?

Abb. 19: Heuristisches „4C“- Bewertungsmodell



Quelle: CAM

„4C“-Modell: Kriterien zur „Messung“ der Qualität der CS-Strategie

Beispielhafte Fragestellungen/Indikatoren
Gibt es umfassende Cyber-Security-Richtlinien?
Sind Strukturpläne und Verfahren zum Erkennen und Reagieren auf CS-Vorfälle sowie des Wiederherstellens nach einem CS-Angriff vorhanden?
Welche Qualität hat das Reporting von CS an den Vorstand? (Detaillierung, Rhythmus)
Wird regelmäßig eine unabhängige Cyber-Sicherheitsrisikobewertung durchgeführt?
Sind alle Vorstände einbezogen in die CS-Diskussionen?
Verfügt der Vorstand über ausreichend Fachwissen, um Anweisungen zur Cybersicherheitsstrategie zu geben und Entscheidungen zur Rechenschaft zu fällen?
Wie ist der Grad der Integration von CS im Unternehmen und als Teils des Risikomanagements?
Wie ist Qualität der Trainingsmaßnahmen der Belegschaft zur Sensibilisierung von CS zu beurteilen?

Abb. 19: Heuristisches „4C“- Bewertungsmodell

Quelle: CAM

Quellenverzeichnis

Quellen

- Baker, R., Köhler, S., Strohmeier, M., & Martinovic, I. (3. März 2023). BROKENWIRE : Wireless Disruption of CCS Electric Vehicle Charging. Abgerufen am 14. September 2023 von https://arxiv.org/pdf/2202.02104.pdf
- BSI (2022): Branchenlagebild Automotive. Cyber-Sicherheit in der Automobilbranche 2021/2022. Zugriff am am 4.07.2023. Online: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Branchenlagebild/branchenlagebild-automotive-2021_2022.html
- BSI (2023): Branchenlagebild Automotive. Cyber-Sicherheit in der Automobilbranche 2022/2023. Zugriff am am 4.07.2023. Online: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Branchenlagebild/branchenlagebild-automotive-2022-2023.html
- Boehner, M. (2019). Security für vernetzte Fahrzeuge entlang des gesamten Lebenszyklus. ATZelektronik, 14 (1–2), 16–21.
- Conti, M., Donadel, D., Poovendran, R., & Turrin, F. (9. September 2022). EVExchange: A Relay Attack on Electric Vehicle Charging System. Von https://labs.ece.uw.edu/nsl/papers/EVExchange_2022.pdf abgerufen
- Curry, Sam (2023): Web-hackers vs. Auto-Industry. Zugriff am 4.07.2023. Online: https://samcurry.net/web-hackers-vs-the-auto-industry/)
- Dalheimer, M. (22. Dezember 2017). Schwarzladen III: Mit USB zum Profit. Abgerufen am 14. September 2023 von gonium.net: https://gonium.net/post/2017-12-22-mit-usb-zum-profit/
- Dalheimer, M. (26. Oktober 2017). Schwarzladen: Ladekarten manipulieren leicht gemacht. Abgerufen am 14. September 2023 von gonium.net: https://gonium.net/post/2017-10-26-schwarzladen/
- Dudek, S. (7. Juni 2019). V2G Injector Whispering to cars and charging units through the Power-Line. Abgerufen am 14. September 2023 von https://www.sstic.org/media/SSTIC2019/SSTIC-actes/v2g_injector_playing_with_electric_cars_and_chargi/SSTIC2019-Slides-v2g_injector_playing_with_electric_cars_and_charging_stations_via_powerline-dudek.pdf
- Ecomento (2023): Neuer VW E-Golf startet frühestens 2028, e-up! läuft 2024 aus. Zugriff am 19.12.2023. Online: https://ecomento.de/2023/04/03/neuer-vw-e-golf-fruehestens-2028-e-up-laeuft-2024-aus/
- ENISA (2021): ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS. Zugriff am 4.07.2023. Online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
- Ermert, M. (22. März 2022). Angriff auf Satellitennetzwerk KA-Sat: Experten suchen nach dem Ursprung. Abgerufen am 14. September 2023 von heise online: https://www.heise.de/news/Angriff-auf-Satellitennetzwerk-KA-Sat-Experten-suchen-nach-dem-Ursprung-6544706.html
- Humphries, M. (2022): Teenage Hacker Gains Remote Control of 25 Teslas in 13 Countries. Accessed on Nov. 14, 2022, at https://www.pcmag.com/news/teenage-hacker-gains-remote-control-of-25-teslas-in-13-countries.
- Huq, N./Gibson, C./Vosseler, R. (2020). Driving Security Into Connected Cars: Threat Model and Recommendations. (Trend Micro Research, Hrsg.) Zugriff am 4.07.2023. Online: *http://documents.trendmicro.com/assets/white_papers/wp-driving-security-into-connected-cars.pdf*
- Huq, N./Gibson, C./Vosseler, R. (2020a). Trend Micro. “The Cybersecurity Blind Spots of Connected Cars.” Accessed on Nov. 14, 2022, at https://documents.trendmicro.com/assets/white_papers/wp-driving-security-into-connected-cars.pdf.

Quellen

- Inf0sec1. (2022): Twitter - “Playing around with #FlipperZero...” Zugriff am 4.07.2023. Online: https://twitter.com/inf0sec1/status/1545804925522829313?t=4-n6SQ3H8OhD_WFXwiLZMg&s=19.
- itemis SECURE 2023: Overview of ISO/SAE 21434. Zugriff am 4.07.2023. Online: https://www.security-analyst.org/inside-the-iso-sae-21434/
- Jadhav, A. (2021): Automotive Cybersecurity. In: M. Kathiresh, R. Neelaveni (eds.): Automotive Embedded Systems. Springer Nature Switzerland.
- Johns, E. (2020): Cyber Security Breaches Survey 2020. Zugriff am 4.07.2023. Online: *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/893399/Cyber_Security_Breaches_Survey_2020_Statistical_Release_180620.pdf*
- *Johnson, W. (30. Januar 2023). Electrify America bug opens hacking vulnerability concerns [Updated]. Von Tesla News, Tips, Rumors and Reviews: https://www.teslarati.com/electrify-america-chargers-hacking-vulnerability-bug/ abgerufen*
- Klapwijk, P., & Driessen-Mutters, L. (November 2018). Exploring the public key infrastructure for ISO 15118 in the EV charging ecosystem. Von https://elaad.nl/wp-content/uploads/downloads/Exploring-the-PKI-for-ISO-15118-in-the-EV-charging-ecoystem-V1.0s2.pdf abgerufen
- Koenen, J. (2021): Hacker legen Autozulieferer EDAG lahm. Zugriff am 4.07.2023. Online: *https://www.handelsblatt.com/unternehmen/industrie/cyberangriff-hacker-legen-autozulieferer-edag-lahm/27005604.html*
- KonBriefing*(2023):* Hackerangriff 2023 in Deutschland aktuell heute. Hacker-Attacken auf Unternehmen und Organisationen. Zugriff am am 4.07.2023. Online: https://konbriefing.com/de-topics/hackerangriff-deutschland.html
- Ladesäulenverordnung § 8 (4). (kein Datum). Verordnung über technische Mindestanforderungen an den sicheren und interoperablen Aufbau und Betrieb von öffentlich zugänglichen Ladepunkten für elektrisch betriebene Fahrzeuge 1. Abgerufen am 14. September 2023 von https://www.gesetze-im-internet.de/lsv/__8.html
- McKinsey 2019 (Johannes Deichmann, Benjamin Klein, Gundbert Scherf, and Rupert Stützle): The race for cybersecurity: Protecting the connected car in the era of new regulation. McKinsey Center for Future Mobility.
- McKinsey 2020 (Ondrej Burkacky, Johannes Deichmann, Benjamin Klein, Klaus Pototzky, Gundbert Scherf): Cybersecurity in automotive. Mastering the challenge. McKinsey Center for Future Mobility (Hrsg.). Zugriff am 4.07.2023. Online: *https://www.gsaglobal.org/wp-content/uploads/2020/03/Cybersecurity-in-automotive-Mastering-the-challenge.pdf*
- McKinsey 2022: The future of automotive computing: Cloud and edge. October (https://www.mckinsey.com/industries/semiconductors/our-insights/the-future-of-automotive-computing-cloud-and-edge)
- Miller, C./ Valasek, C. (2015): Remote Exploitation of an Unaltered Passenger Vehicle. Zugriff am 4.07.2023. Online: http://illmatics.com/Remote%20Car%20Hacking.pdf
- Nio (2022): NIO Becomes the First in China to be Granted UN R155 Cybersecurity Management System Certification, Press Release 25 Januar. Zugriff am 4.07.2023. Online: https://www.nio.com/blog/nio-becomes-first-china-be-granted-un-r155-cybersecurity-management-system-certification
- Nolte, M. (2020): OBD-Schnittstelle: Wie freien Werkstätten der Zugang zu Fahrzeugdaten erschwert wird. Zugriff am am 4.07.2023. Online: *https://herthundbuss.com/branche-mehr/obd-schnittstelle-erschwerter-zugang-fuer-freie-werkstaetten/*

Quellen

- NBC News. (June 16, 2022). YouTube. “Thieves Turning To Cutting Edge Technology To Steal Cars. Zugriff am 4.07.2023. Online: https://www.youtube.com/watch?v=rx5mjOEixMY.
- NCSC (2023): Cyber-Security-Board-Toolkit. Zugriff am 4.07.2023. Online: https://www.ncsc.gov.uk/files/NCSC_Cyber-Security-Board-Toolkit.pdf
- P3 Group 2022 (Autoren: Lucas Bublitz; Alexander Boll; Patrick Eisele; Tobias Löhr; Damian Weinzierl): Automotive Cybersecurity. Cluster Elektromobilität Süd-West, Januar 2022.
- PwC (2023): Global Automotive Cyber Security Management System (CSMS) Survey 2022. Cybersicherheit setzt Automobilbranche unter Druck. Zugriff am 4.07.2023. Online: https://www.pwc.de/de/im-fokus/cyber-security/global-automotive-cyber-security-management-system-survey.html
- Tengler, S. (2020). Top 25 Auto Cybersecurity Hacks: Too Many Glass Houses To Be Throwing Stones, Forbes. Zugriff am 4.07.2023. Online: https://www.forbes.com/sites/stevetengler/2020/06/30/top-25-auto-cybersecurity-hacks-too-many-glass-houses-to-be-throwing-stones/?sh=8a10f2d7f65d
- Toulas, Bill (2022): Bleeping Computer. “General Motors credential stuffing attack exposes car owners info.” Zugriff am 4.07.2023. Online: https://www.bleepingcomputer.com/news/security/general-motors-credential-stuffing-attack-exposes-car-owners-info/
- Red Packet Security (2022): Red Packet Security. “Cuba Ransomware Victim: Etron.” Zugriff am 4.07.2023. Online: https://www.redpacketsecurity.com/cuba-ransomware-victim-etron/.
- UNECE 2021: UN Regulation No. 155. Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. Agreement: 22 January 2021.
- Upstream 2022: Global Automotive Cyber Security Report, Upstream Security Limited
- VDA (2021): Automotive Cyber Security. Recommendation for Cyber Security Interface Agreement (CSIA), with reference to ISO/SAE 21434. Berlin.
- Vector (2022): Automotive Cybersecurity with ISO 21434, CSMS & SUMS, Webinar May 2022. Zugriff am am 4.07.202. Online: https://www.youtube.com/watch?v=NlRw9d_NAr4
- VicOne (2022): Automotive Cybersecurity in 2022. VicOne Report Zugriff am am 4.07.202. Online: https://vicone.com/files/rpt-automotive-cybersecurity-in-2022.pdf
- Vosseler, R., Huq, N., Gibson, C. & Kropotov, V. (2021): Cybersecurity for Connected Cars. Exploring Risks in 5G, Cloud, and Other Connected Technologies. (Trend Micro Research, Hrsg.). Zugriff am am 4.07.2023. Online: https://documents.trendmicro.com/assets/white_papers/wp-cybersecurity-for-connected-cars-exploring-risks-in-5g-cloud-and-other-connected-technologies.pdf
- Westhues, J. (Oktober 2003). Proximity Cards. Abgerufen am 14. September 2023 von cq.cx - Jonathan Westhues: https://cq.cx/prox.pl
- Wikipedia 2023: ISO/SAE 21434. Zugriff am 19.12.2023. Online: https://de.wikipedia.org/wiki/ISO/SAE_21434
- Wittich, Holger 2023: Porsche Macan ab Frühjahr 2024 eingestellt. Zugriff am 19.12.2023. Online: https://www.auto-motor-und-sport.de/verkehr/eu-cybersicherheit-porsche-macan-wird-eingestellt/
- Zastrow, Kai 2022: UNECE regulatory developments on Cybersecurity and OTA NECE regulatory developments on Cybersecurity and OTA.

Anhang

Abbildungsverzeichnis

Tabellen- und Abkürzungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

CS	Cyber Security
CSMS	Cyber Security Management System
EU	European Union
ISO	International Organization for Standardization
KMU	Kleine und mittelständische Unternehmen
OTA	Over-the-air
SAE	Society of Automotive Engineers
UN	United Nations
UNECE	United Nations Economic Commission for Europe
V2X	Vehicle-to-Everything

Impressum und Copyright

Firma
Dr. Bratzel Center of Automotive Management GmbH & Co. KG (CAM)
Director: Prof. Dr. Stefan Bratzel
Responsible for the contents: Prof. Dr. Stefan Bratzel
Authors: Prof. Dr. Stefan Bratzel

Adresse
Center of Automotive Management
An der Gohrsmühle 25
51465 Bergisch Gladbach
Germany

Phone: +49 (0) 22 02 / 2 85 77 - 0
Fax: +49 (0) 22 02 / 2 85 77 - 28
E-Mail: info@auto-institut.de

Disclaimer und Copyright