Cybersicherheit in Fahrzeugen

Herausforderungen und Lösungen für Zulieferer

CATI
Chemnitz Automotive Institute

DiSer Hub

Inhalt

Impressum

Autoren
Dr. Daniel Plorin,
CATI Automotive Institute
c/o TUCed – An-Institut für Transfer und Weiterbildung GmbH
Reichenhainer Straße 29
09126 Chemnitz

Jonas Schatton, M.Sc,
Projektmanager, Dienstleistungsmanagement
FIR e. V. an der RWTH Aachen
Campus-Boulevard 55
52074 Aachen

Lennardt Söhngen, M.Sc,
Projektmanager, Dienstleistungsmanagement
FIR e. V. an der RWTH Aachen
Campus-Boulevard 55
52074 Aachen

Mitwirkende
Martin Schuler,
Projektleiter DiSerHub-Ost

DOI
10.60571/4238

Satz und Design
FIR e. V. an der RWTH Aachen

Bildnachweise
S. 1: © Pixels Hunter – stock.adobe.com
S. 3: © Tangtong – stock.adobe.com
S. 5 und 9: © city of pictures – stock.adobe.com
S. 7: © abdul studio – stock.adobe.com

Lizenzhinweis

Projekt DiSerHub
FIR e. V. an der RWTH Aachen
Campus-Boulevard 55 I 52074 Aachen

E-Mail: projekt-DiSerHub@fir.rwth-aachen.de
diserhub.de

Stand: 11.2025

Zitiervorschlag:
Plorin, D.; Schatton, J.; Söhngen, L.: Cybersicherheit in Fahrzeugen: Herausforderungen und Lösungen. FIR e. V. an der RWTH Aachen, Aachen 2025. DOI: 10.60571/4238

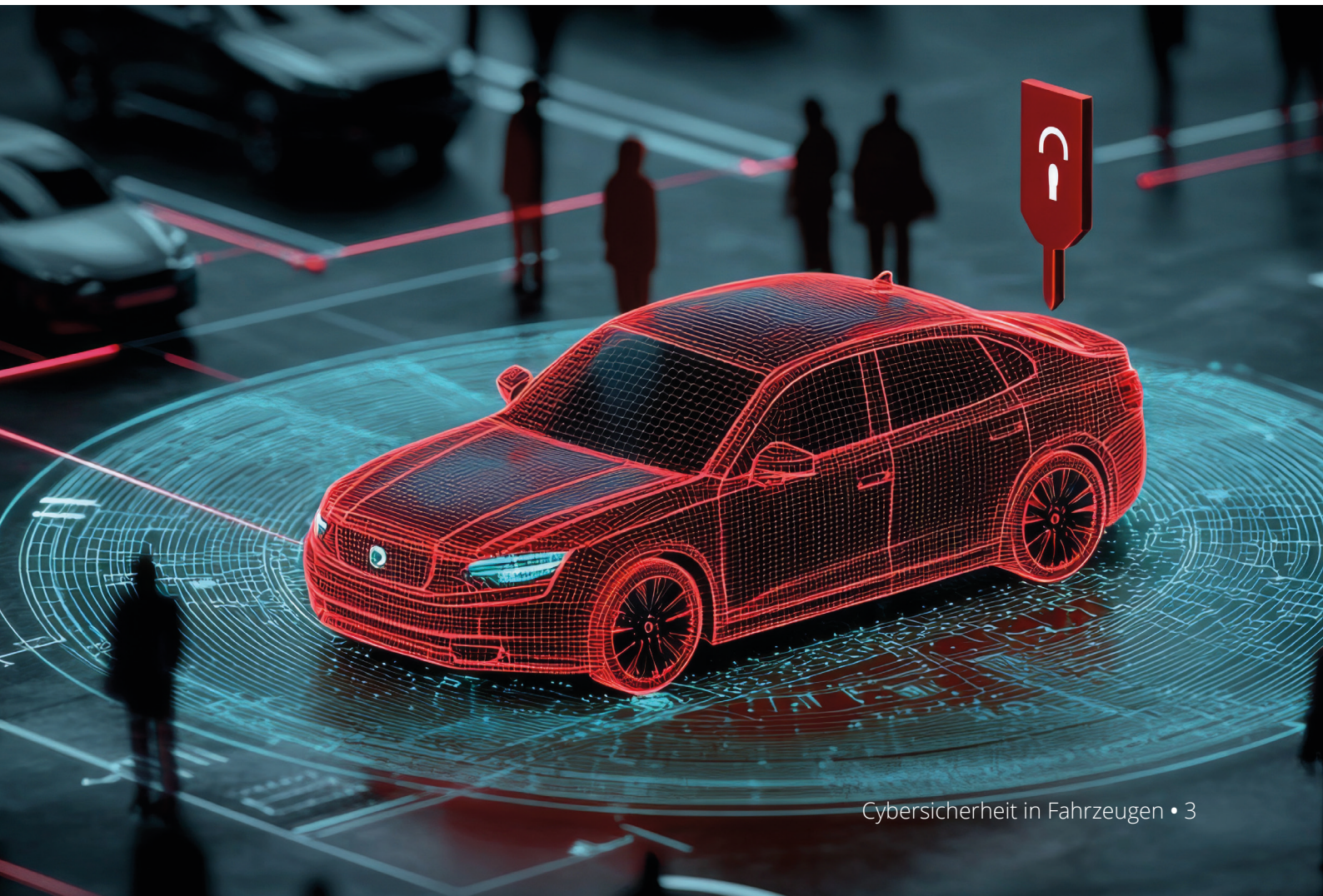
Cybersicherheit in Fahrzeugen

Herausforderungen und Lösungen für Zulieferer

Fahrzeuge sind heutzutage mehr als nur Transportmittel. Sie sind hochkomplexe, vernetzte und I ntelligente Systeme, die eine Vielzahl von Funktionen und Diensten bieten, wie z. B. Navigation, Entertainment, Fahrerassistenz oder teilautonomes Fahren. Diese Funktionen und Dienste basieren auf einer Reihe von Hardware- und Softwarekomponenten, die miteinander kommunizieren, um Daten zu generieren, zu verarbeiten und auszutauschen. Die Vernetzung von Fahrzeugen mit ihrer Umgebung, wie z. B. anderen Fahrzeugen, Infrastrukturen oder Cloud-Diensten, eröffnet neue Möglichkeiten für Innovationen, Effizienz und Komfort, birgt aber auch neue Bedrohungen und Herausforderungen für die Cybersicherheit.

Diese stellt eine große Herausforderung für die Automobilindustrie dar, insbesondere für die Zulieferer, die einen wesentlichen Beitrag zur Entwicklung und Bereitstellung von Fahrzeugkomponenten leisten. Die Zulieferer müssen nicht nur die steigenden technischen Anforderungen an die Sicherheit ihrer Produkte erfüllen, sondern auch die wachsenden regulatorischen Anforderungen an die Sicherheit des gesamten Fahrzeugsystems sowie einzelner Komponenten.

So verlangen etwa die UNECE-Richtlinien R155 und R156, dass alle Neuwagen ab dem 7. Juli 2022 über ein Cybersecurity-Management-System (CSMS) verfü-



gen, das den gesamten Lebenszyklus des Fahrzeugs abdeckt, von der Entwicklung über die Produktion bis hin zur Wartung. Zudem müssen Hersteller einen Prozess der Typgenehmigung durchlaufen, um die Konformität ihrer Fahrzeuge mit den Cybersicherheitsanforderungen nachzuweisen. Diese neuen Vorschriften haben erhebliche Auswirkungen auf die Fahrzeugmodelle und somit auch auf die Zulieferer.

Einige Modelle, wie z. B. der VW Up, der Porsche Boxster/Macan und der VW T6.1, werden aufgrund der hohen Kosten für die Software-Aufrüstung eingestellt. Andere Modelle, die vor dem 7. Juli 2022 auf den Markt kamen, erhalten eine Übergangsfrist bis Sommer 2024, um die neuen Cybersicherheitsstandards zu erfüllen. Diese Modelle müssen jedoch regelmäßig aktualisiert und überwacht werden, um mögliche Schwachstellen oder Angriffe zu erkennen und zu beheben.

Bedrohungen

Ein Bericht von VicOne, ein renommiertes Service- und Beratungsunternehmen speziell zu Cybersicherheit, hebt hervor, dass die Automobilindustrie in der ersten Jahreshälfte Verluste von mehr als 11 Milliarden US-Dollar durch Cyberangriffe erlitten hat, wobei die Lieferkette als Hauptziel identifiziert wurde. Über 90 Prozent dieser Angriffe zielten nicht direkt auf OEMs, sondern auf Zulieferer ab, was die Notwendigkeit unterstreicht, die gesamte Lieferkette zu schützen. Die zunehmende Komplexität der Fahrzeuge, die Nutzung und Monetarisierung von Automobildaten - sowie der Einsatz von Konnektivität und Automatisierung eröffnen neue Angriffsvektoren wie Ransomware und das Eindringen in Backend-Cloud-Infrastrukturen. Zu den dokumentierten Sicherheitslücken gehören unter anderem Out-Of-Bounds-Write (OOBW), Buffer-Overflow und falsche Eingabevalidierungen. Die meisten Schwachstellen finden sich in Chipsätzen und Infotainment-Systemen wieder.

Fahrzeugarchitektur

Die Fahrzeugarchitektur ist einem ständigen Wandel unterworfen, um die steigenden Anforderungen an Leistung, Komplexität und Konnektivität zu erfüllen. Einige der aktuellen Trends in der Fahrzeugarchitektur sind z. B.:

Die **Zentralisierung** oder **Konsolidierung** von *Electronic Control Units* (ECUs), die darauf abzielt, die Anzahl und Vielfalt der ECUs zu reduzieren und stattdessen leistungsstarke und multifunktionale Computerplattformen zu verwenden, die mehrere Anwendungen ausführen können. Dies kann die Effizienz, Flexibilität und Skalierbarkeit der Fahrzeugarchitektur verbessern, aber auch die Angriffsfläche und die Abhängigkeit von einzelnen Komponenten erhöhen.

Die **Virtualisierung** oder **Containerisierung** von Anwendungen, die darauf abzielt, verschiedene Anwendungen in virtuellen Maschinen oder Containern laufen zu lassen, die sich von der Hardware darunter lösen. Dies kann die Anwendungen sicherer, portabler und wiederverwendbarer machen, aber auch mehr Komplexität und Ressourcen verlangen. Ein Container ist ein Softwarepaket, das alles Wichtige zum Ausführen von Software enthält: Code, Laufzeit, Konfiguration und Systembibliotheken.

Die **Cloudifizierung** oder **Edge-Computing von Anwendungen**, die darauf abzielt, die Rechenleistung und den Speicherplatz des Fahrzeugs zu erweitern, indem einige Anwendungen oder Funktionen auf entfernten Servern oder nahegelegenen Geräten ausgeführt werden. Dies kann die Funktionen, Dienste und Updates des Fahrzeugs verbessern, aber auch die Latenz, Bandbreite und Vertraulichkeit beeinträchtigen.

Fahrzeugkomponenten

Die Fahrzeugkomponenten sind die einzelnen Hardware- und Softwareelemente, die die Fahrzeugarchitektur bilden. Diese sind für die Cybersicherheit in Fahrzeugen von großer Bedeutung, da sie die potenziellen Ziele oder Vektoren für Angriffe darstellen. Die wichtigsten Fahrzeugkomponenten aus Sicht der Cybersicherheit sind z. B.:

Die **Sensoren**, die die Daten erfassen, die für die Funktionen und Dienste des Fahrzeugs notwendig sind. Die Sensoren müssen in der Lage sein, genaue, verlässliche und zeitnahe Daten zu liefern, die nicht manipuliert oder gefälscht werden können. Die Sensoren müssen auch vor physischen Schäden oder Sabotage geschützt werden.

Die **Aktuatoren**, die die physischen Aktionen ausführen, die für die Funktionen und Dienste des

Fahrzeugs notwendig sind. Die Aktuatoren müssen in der Lage sein, präzise, konsistente und angemessene Aktionen auszuführen, die nicht blockiert oder umgeleitet werden können. Die Aktuatoren müssen auch vor physischen Schäden oder Sabotage geschützt werden.

Die ECUs, die die Datenverarbeitung, -übertragung und -koordination für die Funktionen und Dienste des Fahrzeugs übernehmen. Die ECUs müssen in der Lage sein, die Integrität, Vertraulichkeit und Verfügbarkeit der Daten zu gewährleisten, die nicht verändert, abgefangen oder unterbrochen werden können. Die ECUs müssen auch vor physischen oder logischen Angriffen geschützt werden, die ihre Funktionsfähigkeit oder Leistung beeinträchtigen oder kompromittieren können.

Die Anwendungen, die die Funktionen und Dienste des Fahrzeugs bereitstellen. Die Anwendungen müssen in der Lage sein, die Korrektheit, Robustheit und Kompatibilität ihrer Funktionen und Dienste zu gewährleisten, die nicht fehlerhaft, anfällig oder inkonsistent sein können. Die Anwendungen müssen auch vor Schadsoftware oder unerwünschter Software geschützt werden, die ihre Funktionen oder Dienste beeinträchtigen oder missbrauchen können.

Die Kommunikationsschnittstellen und -protokolle, die die Kommunikation des Fahrzeugs mit seiner Umgebung ermöglichen. Diese müssen in der Lage sein, die Authentizität, Autorisierung und Verschlüsselung der Kommunikation zu gewährleisten, die nicht gefälscht, abgehört oder manipuliert werden können. Die Kommunikationsschnittstellen und -protokolle müssen auch vor Störungen oder Denial-of-Service(DoS)-Angriffe geschützt werden, die die Kommunikation behindern oder verhindern können.

Fahrzeugfunktionen

Die Fahrzeugfunktionen und -dienste sind die Leistungen, die das Fahrzeug seinen Nutzern bietet. Sie haben einen direkten Einfluss auf die Sicherheit und Zufriedenheit der Nutzer. Die Fahrzeugfunktionen und -dienste sind für die Cybersicherheit in Fahrzeugen relevant, da sie die potenziellen Ziele oder Motive für Angriffe darstellen. Die wichtigsten Fahrzeugfunktionen und -dienste aus Sicht der Cybersicherheit sind...

...die **Navigation**, die dem Nutzer Informationen über den Standort, die Route und die Verkehrsbedingungen liefert. Die Navigation muss in der Lage sein, genaue, aktuelle und relevante Informationen zu liefern, die nicht falsch oder irreführend sind. Die Navigation muss auch vor Störungen oder Umleitungen geschützt werden, die den Nutzer in Gefahr bringen oder vom Ziel abbringen können.

...das **Entertainment**, das dem Nutzer Unterhaltung, Information oder Kommunikation bietet. Das Entertainment muss in der Lage sein, hochwertige, anpassbare und sichere Inhalte zu liefern, die nicht unangemessen oder schädlich sind. Das Entertainment muss auch vor Eingriffen oder Spionage geschützt werden, die die Privatsphäre oder Präferenzen des Nutzers verletzen oder beeinflussen können.

...die Fahrerassistenz, die dem Nutzer Unterstützung, Warnung oder Intervention bei der Fahrzeugsteuerung bietet. Die Fahrerassistenz muss in der Lage sein, effektive, angemessene und vertrauenswürdige Funktionen zu bieten, die nicht fehlerhaft oder gefährlich sind. Die Fahrerassistenz muss auch vor Deaktivierung oder Übernahme geschützt werden, die die Sicherheit oder Kontrolle des Nutzers über das Fahrzeug gefährden oder beeinträchtigen können.

...das autonome Fahren, das dem Nutzer die vollständige oder teilweise Automatisierung der Fahrzeugsteuerung bietet. Das autonome Fahren muss in der Lage sein, sichere, komfortable und konforme Funktionen zu bieten, die nicht unsicher oder illegal sind. Das autonome Fahren muss auch vor Störungen oder Sabotage geschützt werden, die die Sicherheit oder Verantwortung des Nutzers für das Fahrzeug gefährden oder aufheben können.

Regularien

Aktuelle Regularien, die für Zulieferer in der Automobilindustrie hinsichtlich Software und Hardware von Fahrzeugarchitekturen relevant sind, umfassen insbesondere die UN-Regelungen zur Cybersicherheit und Software-Updates. Diese wurden durch die UNECE (Wirtschaftskommission der Vereinten Nationen für Europa) eingeführt und zielen darauf ab, die Risiken zu mindern, die durch die Digitalisierung und Vernetzung von Fahrzeugsystemen entstehen. Die Regelungen umfassen u.a. Bereiche wie sichere Software-Updates: Die Sicherheit der Fahrzeuge darf durch Updates nicht kompromittiert werden, wobei eine rechtliche Grundlage für sogenannte Over-The-Air(OTA)-Updates zur On-Board-Fahrzeugsoftware geschaffen wird.

Die durch diese Regularien adressierten Bedrohungen betreffen eine Vielzahl von Cyberrisiken, die mit der zunehmenden Komplexität elektronischer Systeme in Fahrzeugen und deren Vernetzung mit der Außenwelt zusammenhängen. Hierzu gehören unter anderem das unautorisierte Entriegeln von Türen und Fenstern durch Kriminelle, das Deaktivieren von Sicherheitssystemen kritischer Funktionen und die Beeinträchtigung der Fahrzeugsicherheit und des Datenschutzes der Verbraucher*innen.

Fazit

Die fortschreitende Digitalisierung und Vernetzung von Fahrzeugen bringt neue Herausforderungen im Bereich der Cybersicherheit mit sich. Diese Entwicklung erfordert von der Automobilindustrie und ihren Zulieferern, sich intensiv mit technischen, organisatorischen und rechtlichen Aspekten der Sicherheit auseinanderzusetzen. Fahrzeuge, die zunehmend auf Software, Sensoren, Kommunikationstechnologien und Künstliche Intelligenz angewiesen sind, stellen potenzielle Ziele für Cyberangriffe dar.

Die Herausforderungen sind vielfältig und resultieren aus der Komplexität und Dynamik der Fahrzeugsysteme sowie deren Interaktion mit der Umgebung. Diese umfassen die Vielfalt der potenziellen Angriffsvektoren, die Gewährleistung der Sicherheit über den gesamten Lebenszyklus der Fahrzeugsysteme, die Abhängigkeit von externen Partnern und Dienstleistern, die Anpassung an sich ändernde Bedrohungen und die Einhaltung gesetzlicher sowie regulatorischer Anforderungen. Zudem beeinflussen Trends wie zunehmende Automatisierung und Autonomie, wachsende Konnektivität und Interoperabilität, steigende Digitalisierung und Software-Intensität, Diversifizierung und Personalisierung von Fahrzeugen sowie eine verstärkte Sensibilisierung und Regulierung die Entwicklung und den Betrieb von Fahrzeugen.

Für Zulieferer in der Automobilindustrie ergeben sich aus diesen Herausforderungen nicht nur Anforderungen, sondern auch Chancen. Sie sind gefordert, Hardware- und Software-Komponenten zu entwickeln, die den hohen Sicherheitsanforderungen gerecht werden und die Sicherheit der Fahrzeugsysteme über deren gesamten Lebenszyklus sicherstellen. Dies erfordert eine enge Zusammenarbeit mit Automobilherstellern und anderen Zulieferern, die Einhaltung von Standards und Best Practices sowie eine kontinuierliche Anpassung an neue Sicherheitsbedrohungen. Zugleich können sich Zulieferer als kompetente und vertrauenswürdige Partner im Bereich der Cybersicherheit positionieren und von der steigenden Nachfrage nach sicheren, vernetzten und automatisierten Fahrzeugen profitieren.

Literatur

CATI-Quellen

Als CATI-Quellen dienten diverse Projektberichte zur Automobilzulieferindustrie in Sachsen (2016 und 2019) und in Thüringen (2018 und 2022) mit den jeweiligen Kapiteln zu aktuellen Trends und Strategien in der Automobilindustrie (Prof. Dr. Werner Olle und Dr. Daniel Plorin). Bei näherem Interesse an den Quellen wenden Sie sich gern ans CATI.

Weiterführende Informationen

Baumann, F.: Softwarecontainer: Standardisierung ist der Schlüssel . Springer Professional, 28.03.2024. https://www.springer-professional.de/automobilelektronik---software/funktionale-sicherheit/softwarecontainer--standardisierung-ist-der-schluessel/26828178 (Link zuletzt geprüft: 06.11.2025)

Bretting, R.: UNECE WP.29 setzt neue Standards: Mehr Cybersicherheit für vernetzte Fahrzeuge. automotiveIT online, 17.05.2021. https://www.automotiveit.eu/strategy/mehr-cybersicherheit-fuer-vernetzte-fahrzeuge/899718 (Link zuletzt geprüft: 06.11.2025)

dpa (Hrsg.): [Pressemitteilung]Reaktion auf Vorschriften der EU: Volkswagen streicht Modelle wegen Cybersecurity-Vorgaben. automotiveIT online, 19.03.2024. https://www.automotiveit.eu/technology/volkswagen-streicht-modelle-wegen-cybersecurity-vorgaben/923053 (Link zuletzt geprüft: 06.11.2025)

Dudemaine, R.: Entscheidend ist die Betriebssystemarchitektur: Leistungsfähigkeit und Sicherheit von E-Fahrzeugen optimieren. All electronics online, 31.08.2021. https://www.all-electronics.de/e-mobility/leistungsfaehigkeit-und-sicherheit-von-efahrzeugen-optimieren/753349 (Link zuletzt geprüft: 06.11.2025)

Gomoll, W.: Cybersecurity für Autos: Gefährliche Sicherheitslücken. automotiveIT online, 03.02.2021. https://www.automotiveit.eu/technology/gefaehrliche-sicherheitsluecken/907916 (Link zuletzt geprüft: 06.11.2025)

Hammerschmidt, C.: Zahlreiche Risikofaktoren: Cybersecurity benötigt eine ganzheitliche Sicherheitskultur. automotiveIT online, 13.01.2021. [in Bibliothek des FIR e. V. an der RWTH Aachen verfügbar]

Hochwarth, D.: Aufrüstung würde Millionen kosten: Neue EU-Regeln für Cybersecurity bei Neuwagen lassen Modellpalette schrumpfen. VDI online, 19.03.2024. https://www.vdi-nachrichten.com/technik/automobil/neue-eu-regeln-fuer-cybersecurity-bei-neuwagen-lassen-modellpalette-schrumpfen/ (Link zuletzt geprüft: 06.11.2025)

Klische, M.: Cyber Security in Fahrzeugen: Wettlauf zwischen Hackern und Industrie. heise online, 06.10.2023. https://www.heise.de/hintergrund/Cyber-Security-in-Fahrzeugen-Wettlauf-zwischen-Hackern-und-Industrie-9318721.html (Link zuletzt gerüft: 06.11.2025)

Köllner, C.: Diese Cyberrisiken bedrohen die Automobilindustrie. Springer Professional, 23.01.2024. https://www.springerprofessional.de/cyber-sicherheit/automobilwirtschaft/diese-cyberrisiken-bedrohen-die-automobilindustrie/26598942 (Link zuletzt geprüft: 06.11.2025)

Lorenz, M.: Cybersicherheit: Fundament für autonomes Fahren. VDA online, o. D. https://www.vda.de/de/themen/digitalisierung/daten/cybersicherheit (Link zuletzt geprüft: 06.11.2025)

Stawski, M.: Automotive Cybersecurity: Ein umfassender Leitfaden. newdigitalstreet online, 20.11.2023. https://newdigitalstreet.com/de/automotive-cybersecurity/ (Link zuletzt geprüft: 06.11.2025)

SWR-Onlinered. (Hrsg.): Modell erfüllt neue Vorgaben nicht: Porsche stoppt Verkauf des Macan mit Verbrenner in der EU. SWR online, 14.12.2023. https://www.swr.de/swraktuell/baden-wuerttemberg/porsche-stoppt-verkauf-macan-eu-100.html (Link zuletzt geprüft: 06.11.2025)

vicOne (Hrsg.): Automotive Cybersecurity Report 2023; erschienen in drei separaten Teilen: Fahrzeugdaten: Chancen, Monetarisierung und Cybersecurity-Bedrohungen bei vernetzten Fahrzeugen; VicOne Automotive Cyberthreat Landscape Report 2023; VicOne Automotive Cybersecurity-Prognosen für 2024. Tokio [u. a.] 2023. https://vicone.com/de-reports/automotive-cybersecurity-report-2023#downloads (Link zuletzt geprüft: 18.11.2025)

Wenzel, F.-T.: Auf Wiedersehen VW Bulli T6: Der Aufwand lohnt nicht mehr: Wie der Schutz vor Hackerangriffen das Ende beliebter Autos besiegelt. RND online, 19.03.2024. https://www.rnd.de/wirtschaft/vw-up-porsche-boxter-vw-t6-1-warum-die-cybersicherheit-das-ende-beliebter-pkw-besiegelt-JHATGE3IJFABFNW4DJODRSP5WE.html (Link zuletzt geprüft: 06.11.2025)

DiSer Hub

Zuwendungsgeber:

Gefördert durch:

Bundesministeriur für Wirtschaft und Energie

Förderkennzeichen: 16THB0004A
Laufzeit: 01.09.2022 – 31.12.2025
Projektträger:

VDI | VDE | IT

VDI / VDE Innovation + Technik GmbH

5 Partner. 5 Standorte. 1 Netzwerk.

fir an der RWTH Aachen

Fraunhofer AUTOMOBIL

ifa Institut für Automobilwirtschaft

SICP Software Innovation Campus Paderborn
HEINZ NIXDORF INSTITUT UNIVERSITÄT PADERBORN

TECHNISCHE UNIVERSITÄT CHEMNITZ

TUCed AN-INSTITUT FÜR TRANSFER UND WEITERBILDUNG

diserhub.de