Digitale Revolution im Automobilsektor: IT-Sicherheitsimperative für Zulieferer

IT-Sicherheitsmanagement für das softwarebasierte Fahrzeug

Fabian Meyer
Marian Matthies
Muskaan Multani

Dezember 2023
Blogpost

Key Facts

- Innovationsantrieb durch ACES-Disruptionen: Die Automobilindustrie erfährt durch autonome Fahrzeuge, Vernetzung, Elektromobilität und Shared Mobility einen Innovationsschub, der die Rolle von Softwarekomponenten verstärkt.
- In den letzten Jahren wurde ein signifikanter Anstieg von Cyberangriffen verzeichnet, was die Notwendigkeit sicherer Software in der Automobilindustrie unterstreicht.
- Die Automobilindustrie sieht sich mit strengen regulatorischen und normativen Anforderungen konfrontiert, darunter UNECE WP.29 R155 und R156, ISO/SAE 21434, ISO 24089, ISO/IEC 27001 und TISAX.
- Zulieferer stehen vor der Herausforderung, diese umfangreichen Anforderungen effizient und ressourcenschonend umzusetzen, während sie den OEM-Anforderungen gerecht werden.
- Ein strukturierter und systematischer Ansatz für Sicherheitsvorgaben fördert die langfristige Einhaltung dieser Vorgaben auf verschiedenen Ebenen und unterstützt Effizienz sowie Adaptibilität.
- Harmonisierung von Hardware- und Software-Sicherheitskonzepten: dies beinhaltet die Identifizierung, Bewertung und Minderung von Risiken über den gesamten Fahrzeuglebenszyklus und deckt funktionale Sicherheit, Fahrzeugsicherheit, IT-Sicherheit, Umweltsicherheit und Notfallreaktionen ab.
- Zukunftsorientierte Sicherheitsstrategie mit Kundeneinbindung: Die Entwicklung einer zukunftsgerichteten Sicherheitsstrategie, inspiriert, unter anderem von der Finanzbranche sowie die aktive Einbeziehung der Endkunden, stärkt das Sicherheitsbewusstsein und die Verantwortung.

Steuerung in die Zukunft - Wie die Automobilbranche in das Land der Technologie navigiert

Stellen Sie sich vor, Sie fahren auf einer belebten Autobahn, und plötzlich übernehmen unsichtbare Hände die Kontrolle über Ihr Fahrzeug. Ein fiktives Szenario? Keineswegs. Dies ist bereits Realität, wo Autos zu fahrenden Computern geworden – und somit auch anfällig für Hacks und Cyberangriffe sind. In einem Experiment, das von WIRED durchgeführt wurde, übernahmen Hacker erfolgreich die Kontrolle über einen Jeep Cherokee. Sie manipulierten nicht nur die Scheibenwischer und das Soundsystem, sondern brachten das Auto auch auf einem vielbefahrenen Highway zum Stillstand und lenkten es sogar in einen Graben.[1] Wie kann so ein Szenario verhindert werden und wie können Automobilhersteller hier entgegenwirken und sicherstellen, dass dies ausgeschlossen wird? Während für Hardware-Komponenten durch zahlreiche Regulierungen und Erfahrungen entsprechende Sicherheitsmaßnahmen und Best Practices etabliert wurden, ist die Handhabung der Bedrohungen in Bezug auf Software eine Herausforderung, die es noch zu meistern gilt – vor allem auch, wenn Software und Hardware als Teil von elektrischen und elektronischen Komponenten (E/E) zusammentreffen.

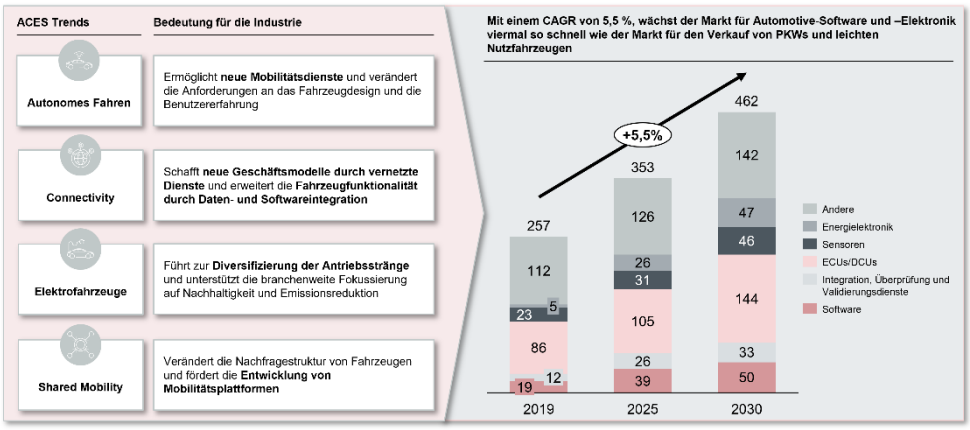

Abbildung 1: ACES Disruptionen im Automotive-Sektor führen zu einem rasanten Wachstum für Automotive-Software und Elektronik

In den letzten Jahren haben vier ACES-Disruptionen, nämlich autonomes Fahren, vernetzte Autos, Elektrofahrzeuge und gemeinsame Mobilität die Agenda der Führungskräfte in der Automobilindustrie dominiert. Mit dem rasanten Fortschritt der Technologie und der Digitalisierung des Autos sind Software Komponenten heute bereits und werden auch in Zukunft zu den grundlegenden Innovationen in modernen Fahrzeugen zählen. Dies eröffnet der Automobilbranche zahlreiche Chancen. Der globale Markt für Automotive-Software und -Elektronik wird bis 2030 voraussichtlich ein Volumen von 462 Milliarden US-Dollar erreichen. Dies entspricht einer jährlichen Wachstumsrate von 5,5 Prozent zwischen 2019 und 2030. Der Automobilsoftware-Markt allein wird sich voraussichtlich mehr als verdoppeln, von 31 Milliarden US-Dollar im Jahr 2019 auf etwa 80 Milliarden US-Dollar im Jahr 2030, und zeigt damit die zunehmende Bedeutung von Softwarekomponenten in Fahrzeugen.[2] Diese Entwicklung wird auch durch den Fortschritt im Bereich des autonomen Fahrens vorangetrieben. Es wird erwartet,

[1] https://www.adac.de/rund-ums-fahrzeug/ausstattung-technik-zubehoer/autonomes-fahren/recht/autonomes-fahren-hacker-angriff/
[2] https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/mapping-the-automotive-software-and-electronics-landscape-through-2030

dass bis 2030 etwa 12 Prozent der Fahrzeuge mit autonomen Fahrfähigkeiten ausgestattet sein werden.[3]

Ein erhöhter Automatisierungsgrad führt jedoch auch zu erhöhter Komplexität im Fahrzeug und steigenden Aufgaben bei den Systemeigenschaften, welches wiederum steigende Sicherheitsanforderungen und potenziellen Schwachstellen mit sich zieht, die durch die zunehmende Vernetzung und die Integration fortschrittlicher Softwaretechnologien in Fahrzeugen entstehen. Ein durchschnittliches Luxusauto enthält, mit circa 100 Millionen Codezeilen, heute mehr Codezeilen als die Boeing 787 Dreamliner[4], der F-35 Joint Strike Fighter und der F-22 Raptor zusammen. Diese Menge an Code ist der Motor, der die Automobilindustrie vorantreibt. Allerdings birgt sie auch Risiken indem sie neue Schwachstellen und IT-Sicherheitsrisiken hervorbringen kann.

Beispielsweise ist laut einem Bericht von Upstream Security die Anzahl der Angriffe auf Automotive Programmierschnittstellen (Application Programming Interfaces / APIs) im Jahr 2022 um 380 Prozent gestiegen und macht dabei nun 12 Prozent aller Vorfälle aus.[5] APIs sind entscheidend für datengetriebene Dienste und fortschrittliche Funktionen, stellen durch ihre Offenheit gleichzeitig aber auch bedeutende Angriffsvektoren dar.

Parallel dazu entwickelt sich das Bewusstsein der Kunden weiter. Sie sind heute mehr denn je über Security-Themen informiert, was auch auf die zahlreichen Berichte über Hackerangriffe zurückzuführen ist, wie zum Beispiel der Hack eines Tesla Model X durch einen mit einem Wi-Fi-Dongle ausgestatteten Drohne innerhalb von 40 Minuten und der Diebstahl von 43 Autos mit schlüssellosen Einstiegssystemen in Columbus, Ohio, durch Simulation von Signalen von Autoschlüsseln.

Daher hat sich die IT-Sicherheit in der Fahrzeugtechnologie zu einem zentralen Differenzierungsmerkmal entwickelt, das neben den etablierten Verkaufsargumenten steht und im Zulassungsprozess unabdinglich ist. Der steigende Bedarf an digitalen Produkten und Services erfordert ein proaktives Vorgehen von Automobilherstellern und Zulieferern, um die Sicherheit der Kunden zu gewährleisten. Es besteht ein dringender Bedarf an starken Risikomanagement-Maßnahmen und geeigneten Prozessen für die Rechtssicherheit diesbezüglich. Ein starker Fokus auf IT-Sicherheit ist daher unabdingbar, um das Vertrauen der Kunden zu gewinnen und zu erhalten.

Zulieferer im Fokus – Verständnis schaffen für die steigenden Sicherheitsrisiken und Anforderungen der Automobilhersteller

Das durchschnittliche Auto enthält mehr als hundert elektronische Steuereinheiten (electronic control units oder kurz: ECUs), die diverse Arten von Software ausführen. Hacker können jede dieser Einheiten angreifen. Cyberkriminelle konzentrieren sich jedoch hauptsächlich auf die

[3] https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/mapping-the-automotive-software-and-electronics-landscape-through-2030

[4] https://newsroom.porsche.com/de/2021/innovation/porsche-engineering-wenn-software-software-schreibt-23325.html

[5] https://upstream.auto/reports/global-automotive-cybersecurity-report/

Fahrzeugteile, die ihnen Zugang zu wertvollen Daten gewähren oder die vollständige Kontrolle über das gesamte Fahrzeug ermöglichen.

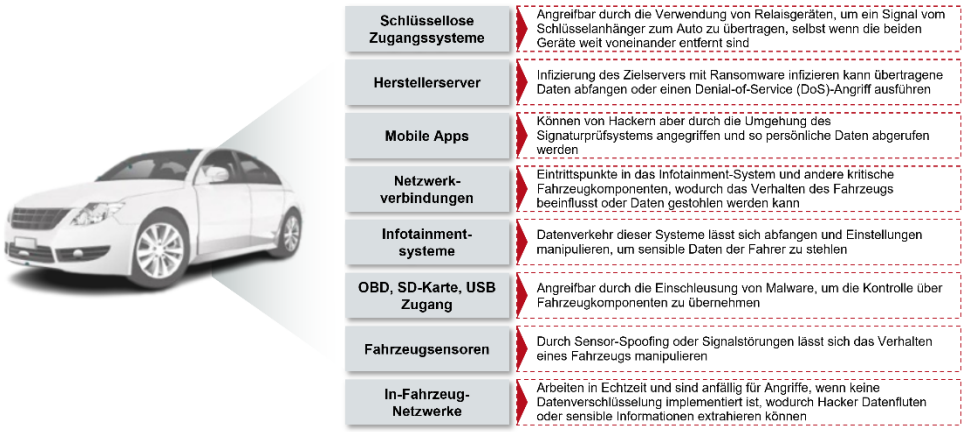

Abbildung 2: Für Hackerangriffe vulnerable Stellen im Fahrzeug

Schlüssellose Zugangssysteme sind laut Schätzungen mittlerweile für 48 Prozent der Fahrzeugdiebstähle verantwortlich,[6] da sie durch Signalverstärkung von Dieben überlistet werden können. Mobile Apps erhöhen zwar den Komfort, sind jedoch anfällig für Cyberangriffe, die persönliche Daten gefährden. Herstellerserver fungieren als zentrale Kommunikationsknoten und locken Hacker an, die möglicherweise Dienste unterbrechen oder Daten entwenden wollen. Fahrzeugsensoren und Infotainment-Systeme können manipuliert werden, um Fahrverhalten zu beeinflussen oder Nutzerdaten zu entwenden. Netzwerkverbindungen und Fahrzeugnetzwerke sind potenzielle Einfallstore für Cyberattacken, während physische Schnittstellen wie On-Board-Diagnose Ports (OBD-Ports), obwohl weniger gefährdet, bei Missbrauch erheblichen Schaden verursachen können.

Datenverletzungen sind auf dem Vormarsch und machen nun 37 Prozent der Cybersicherheitsvorfälle in der Automobilindustrie aus.[7] Die steigende Vernetzung der Fahrzeuge hat auch die Anzahl der identifizierten Schwachstellen erhöht, was die Notwendigkeit von robusten Sicherheitsprotokollen unterstreicht. Insbesondere Angriffe auf Backend-Server, die 40 Prozent aller Angriffe ausmachen, haben zugenommen.[8] Dies betont die Wichtigkeit von sicheren Serverinfrastrukturen. Die dokumentierten Hackerangriffe auf Fahrzeuge haben ebenfalls zugenommen, was ein weiteres Alarmsignal für die Branche darstellt. Recherchen heben auch die steigende Bedeutung der Software Bill of Materials (SBOM) hervor, die eine entscheidende Rolle bei der Verbesserung der Bedrohungsintelligenz in der Automobilindustrie spielt.[9]

Um diese Risiken zu addressieren und zu mitigieren, stellen Automobilhersteller zunehmend ihre Zulieferer in die Pflicht, entsprechende Sicherheitsgarantien in den Lieferantenverträgen abzugeben. Die meisten Automobilhersteller verfügen aber nicht über die notwendigen Softwareentwicklungsfähigkeiten. Sie sind in der Regel nur dafür verantwortlich, die Systemintegration vorzunehmen, während der Rest in der Verantwortung der Zulieferer liegt. Aufgrund des Fehlens

[6] https://www.lv.com/insurance/press/keyless-technology-drives-rise-in-theft-over-past-four-years

[7] https://upstream.auto/reports/h1-2023-automotive-cyber-trend-report/

[8] https://upstream.auto/reports/h1-2023-automotive-cyber-trend-report/

[9] https://upstream.auto/reports/h1-2023-automotive-cyber-trend-report/

robuster Fähigkeiten in Automobilproduktionsstätten und Servicezentren erhöht sich die Zeitverzögerung bei der Behebung identifizierter Schwachstellen. Die Entwicklung von Sicherheitscode-Updates ist aufgrund von Backend-Systemdatensätzen ein zeitaufwendiger Prozess, der den gesamten Prozess der Lieferung von Updates an den Markt ohne Verzögerung beeinträchtigt. Die Verantwortung für sichere Komponenten und Systeme liegt demnach zu einem großen Teil bei den Zulieferern. Bei einer Fertigungstiefe (Anteil der Eigenproduktion von Herstellern am Endprodukt) von durchschnittlich 30 Prozent und dementsprechend 70 Prozent Fremdproduktion ist die Rolle der Zulieferer für sichere Software erheblich und somit auch zwingend zu adressieren.[10]

Zulieferer betreten unfamiliäres Territorium durch die regulatorischen und normativen Anforderungen

In der Automobilindustrie haben strenge regulatorische und normative Anforderungen und umfangreiche Erfahrungen zu erheblichen Fortschritten in der Fahrzeugsicherheit geführt.

Als Teil der Fahrzeugsicherheit, ist die IT-Sicherheit wiederum ein relativ neues Feld, dass sich noch in den Anfangsphasen der Anpassung an neue regulatorische und normative Herausforderungen befindet. Es ist nicht direkt möglich, bewährte Sicherheitsprozesse aus dem Non-IT-Bereich einfach auf die Software-Komponenten zu übertragen. IT-Sicherheit erfordert spezifische Überlegungen, wie den Schutz vor Malware, die Sicherheit von Datenübertragungen und die Gewährleistung der Integrität von Software-Updates.

Gesetzgeber haben die Risiken erkannt und arbeiten daran, regulatorische Lücken zu schließen, indem sie neue Anforderungen an die Industrie stellen. In den letzten Jahren hat sich die Automobilbranche in einem sich wandelnden regulatorischen Umfeld wieder gefunden, geprägt von zunehmenden regulatorischen Anforderungen wie der UNECE WP.29 R155 und R156 Regulierung und normativen Anforderungen wie der ISO/SAE 21434 für Cybersecurity-Management-Systeme (CSMS) und der ISO 24089 für Software-Updates. Daneben existieren zahlreiche weitere Standards wie etwa der ISO/IEC 27001 für Informationssicherheitsmanagementsysteme (ISMS) oder das für die Autobranche spezifische TISAX-Zertifikat. Dadurch, dass ein Großteil der Verantwortung bei den Zulieferern liegt, sind diese also gefragt, die regulatorischen Anforderungen zu meistern, während sie gleichzeitig auch den (überschneidenden) Anforderungen der Automobilhersteller aus den Lieferantenverträgen gerecht werden müssen. Das heißt für Zulieferer, dass sie neben den regulatorischen Anforderungen auch Marktanforderungen gerecht werden müssen, um wettbewerbsfähig zu sein. Zulieferer stehen vor der Herausforderung, einen Gleichgewichtsakt zu bewältigen, indem sie versuchen, alle Anforderungen effizient und ressourcenschonend zu erfüllen und umzusetzen.

[10] https://www.faz.net/aktuell/wirtschaft/unternehmen/autohersteller-und-zulieferer-verbunden-auf-gedeih-und-verderb-14402472.html

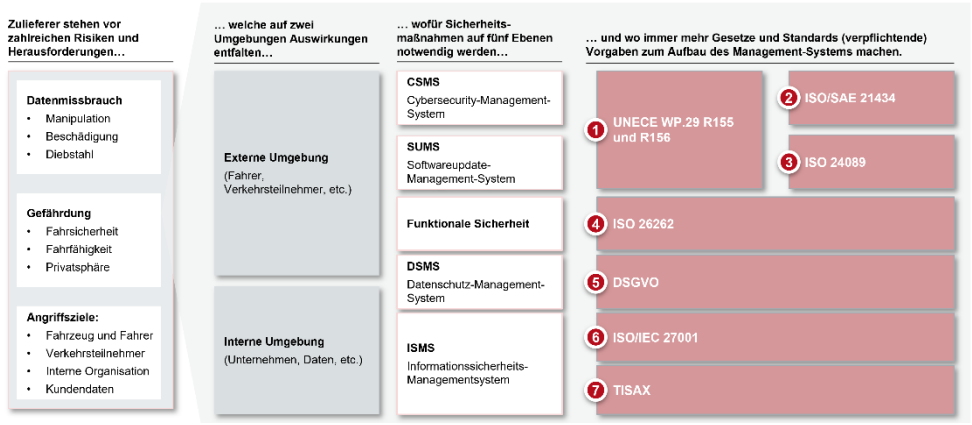

Abbildung 3: Überblick über Kategorisierung von IT-Sicherheitsmaßnahmen

Die relevantesten Rahmenwerke sind hierbei:

1. **WP.29 R155 und R156:** Die WP.29-Regulierung R155 und R156 zu Cybersecurity und Softwareupdates ist eine Initiative der UNECE (United Nations Economic Commission for Europe), die eine führende Rolle in der Entwicklung und Implementierung internationaler Standards für Fahrzeugsicherheit und -zuverlässigkeit spielt. Diese Regulierung zielt darauf ab, die wachsenden Risiken von Cyberangriffen in der Automobilindustrie zu adressieren. Die UNECE setzt sich dafür ein, dass Hersteller effektive Schutzmaßnahmen gegen Cyberbedrohungen implementieren und regelmäßige Softwareupdates durchführen, um die Sicherheit und Funktionalität der Fahrzeuge zu gewährleisten. Die Vorschriften beinhalten Richtlinien für die ständige Überwachung von Fahrzeugsystemen und eine schnelle Reaktion auf identifizierte Sicherheitsrisiken. Diese Maßnahmen sind entscheidend, um ein hohes Maß an Sicherheit und Zuverlässigkeit in modernen Fahrzeugen sicherzustellen. Auch wenn nicht explizit erwähnt, gibt es große Überschneidungen zwischen dieser Regulierung und den beiden Normen ISO/SAE 21434 und ISO 24089.

2. **ISO/SAE 21434:** Die ISO/SAE 21434 ist eine Norm, die ingenieurtechnische Anforderungen für das Cybersecurity-Risikomanagement in Bezug auf Konzeption, Produktentwicklung, Produktion, Betrieb, Wartung und Stilllegung von E/E Systemen in Straßenfahrzeugen, einschließlich ihrer Komponenten und Schnittstellen, spezifiziert. Sie definiert einen Rahmen, der Anforderungen an Cybersecurity-Prozesse und eine gemeinsame Sprache für die Kommunikation und das Management von Cybersecurity-Risiken umfasst. Die Norm legt besonderen Wert auf zwei Hauptfaktoren bei der Bewertung eines Risikos: die Wahrscheinlichkeit eines Angriffs und die potenziellen Auswirkungen einer solchen Attacke. Ein neues Konzept, das durch diesen Standard eingeführt wird, ist das der „Cybersecurity Assurance Level“ (CAL). Dieses Konzept ermöglicht es, zu bestimmen, wie umfassend ein bestimmtes System gegen Angriffe geschützt werden muss. Unternehmen können ihre Cybersecurity-Maßnahmen basierend auf dem CAL anpassen, indem sie je nach festgelegtem CAL-Wert strengere oder weniger strenge Sicherheitsmaßnahmen umsetzen. Für Zulieferer der Automobilhersteller ist diese Norm besonders bedeutsam, da sie die Verantwortung für die Implementierung robuster Cybersecurity-Maßnahmen in den von ihnen gelieferten Komponenten und Systemen tragen. Die Norm ist anwendbar auf E/E-

Systeme von Serienproduktionsstraßenfahrzeuge, deren Entwicklung oder Modifikation nach der Veröffentlichung des Standards begonnen hat. Sie schreibt keine spezifische Technologie oder Lösungen im Zusammenhang mit Cybersecurity vor, bietet jedoch eine klare Richtlinie für die Entwicklung und Implementierung von Cybersecurity-Maßnahmen in der Automobilindustrie.

3. **ISO 24089:** Anders als der Cybersecurity-Standard nimmt der Standard direkt nur OEMs in die Pflicht, da er sich auf Anforderungen für die Implementierung sicherer Updates sowie die Anwendung von Fahrzeugsoftware und zugehörigen Engineering-Aktivitäten konzentriert. Diese Norm fordert von den OEMs, spezifische Prozesse und Methoden sowohl auf organisatorischer als auch auf Projektebene zu etablieren. Sie müssen Anforderungen in Bezug auf die Infrastruktur für Software-Updates, die Fahrzeug- und Fahrzeugsystementwicklung, sowie die Erstellung und Validierung von Software-Update-Paketen und die Durchführung von Software-Updates erfüllen. Dies betont die Notwendigkeit robuster Entwicklungsprozesse für Fahrzeuge und Software sowie effizienter unterstützender Strukturen und Prozesse bei den Fahrzeugherstellern. In Folge werden hierdurch also auch Anforderungen der OEMs an ihre Zulieferer generiert.

4. **ISO 26262:** Die ISO 26262 beinhaltet Anforderungen für den gesamten Lebenszyklus von Fahrzeugen, von der Konzeptphase bis zur Außerbetriebnahme, und berücksichtigt verschiedene Aspekte wie die Entwicklung, Implementierung, Integration und Validierung sicherheitsrelevanter elektronischer Systeme. Sie beinhaltet auch Richtlinien zur Qualifikation von Hardware und Software, die in Fahrzeugen verwendet werden. Die Norm legt besonderen Wert auf die systematische Identifizierung und Bewertung von Risiken, die mit potenziellen Fehlfunktionen elektronischer Systeme in Fahrzeugen verbunden sind. Dies umfasst die Definition von Sicherheitszielen und die Entwicklung von Maßnahmen zur Risikominderung. Der Standard fordert eine gründliche Analyse und Bewertung der Sicherheitsrisiken in jeder Phase der Entwicklung und Produktion, um sicherzustellen, dass die Systeme die festgelegten Sicherheitsanforderungen erfüllen.

5. **DSGVO:** Automobilhersteller und Zulieferer sammeln, verarbeiten und speichern große Mengen an personenbezogenen Daten, beispielsweise durch vernetzte Fahrzeuge, Kundeninteraktionen und digitale Dienste. Die DSGVO verlangt von diesen Unternehmen, dass sie transparent darüber informieren, wie sie diese Daten verwenden, und dass sie die Zustimmung der betroffenen Personen für die Datenerhebung und -verarbeitung einholen. Darüber hinaus müssen Automobilunternehmen sicherstellen, dass die gesammelten Daten sicher aufbewahrt und vor unbefugtem Zugriff geschützt werden. Im Falle eines Datenlecks sind sie verpflichtet, dies innerhalb einer bestimmten Frist den Aufsichtsbehörden und den betroffenen Personen zu melden.

6. **ISO/IEC 27001:** Die ISO/IEC 27001 ist eine international anerkannte Norm, die die Anforderungen für ein ISMS festlegt. Sie konzentriert sich auf den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen in einem Unternehmen durch die Anwendung eines risikobasierten Ansatzes. Die ISO/IEC 27001 ist branchenunabhängig und für jede

Organisation anwendbar, die ihre Informationssicherheit verbessern möchte. Während ein Cybersecuritymanagementsystem auf den Schutz der Verkehrsteilnehmer und Bevölkerung abzielt, dient ein ISMS vor allem dem Schutz der Organisation. ISO/SAE 21434 und ISO/IEC 27001 verfolgen also verschiedene Ziele, haben thematisch und von den Anforderungen aber große Überschneidungen.

7. **TISAX:** TISAX (Trusted Information Security Assessment Exchange) ist ein Standard für Informationssicherheit, der speziell für die Automobilindustrie entwickelt wurde. Es handelt sich um ein Zertifizierungsschema, das auf der ISO/IEC 27001 basiert und von der European Network Exchange (ENX) Association verwaltet wird. TISAX erweitert die ISO/IEC 27001-Norm, indem es zusätzliche Anforderungen im Bereich Datenschutz und Prototypenschutz integriert. Der Standard ermöglicht es Automobilherstellern und ihren Zulieferern, die Effektivität ihrer Informationssicherheitsmaßnahmen zu bewerten und zu validieren. Für Automobilzulieferer ist das TISAX-Zertifikat von erheblicher Bedeutung, da es oft eine Voraussetzung ist, um Geschäfte mit OEMs aufzunehmen und aufrechtzuerhalten. Durch das Erreichen und Aufrechterhalten der TISAX-Zertifizierung können Zulieferer nachweisen, dass sie die notwendigen Sicherheitskontrollen und -praktiken implementiert haben, um die Vertraulichkeit und Integrität der von ihnen verwalteten sensiblen Informationen zu schützen. TISAX fördert auch die Standardisierung der Informationssicherheitsbewertungen in der Automobilindustrie, indem es ein gemeinsames Bewertungs- und Austauschverfahren bietet. Dies erleichtert den Informationsaustausch zwischen Zulieferern und OEMs und reduziert die Notwendigkeit mehrfacher Bewertungen, was zu einer effizienteren und konsistenteren Bewertung der Informationssicherheit führt.

Daneben gibt es noch zahlreiche allgemeine Gesetze, aus denen sich Anforderungen für Zulieferer ergeben, wie etwa zum Datenumgang aus der DSGVO sowie zahlreiche Best Practices und Rahmenwerke, wie die Automotive ISAAC Best Practices oder die Guidelines on National Intelligent Manufacturing.

Legt man die verschiedenen Dokumente der Regularien und Standards übereinander, lassen sich inhaltlich viele Gemeinsamkeiten erkennen. Beispielsweise unterstreichen die Standards die Notwendigkeit einer systematischen Risikobewertung, bei der Risiken identifiziert, analysiert und priorisiert werden. Die Etablierung eines Risikobehandlungsprozesses, einschließlich der Festlegung von Kontrollen und der Formulierung eines Risikobehandlungsplans, ist hierbei zentral. Im Bereich der Organisation und Governance wird von den Unternehmen erwartet, dass sie relevante interne und externe Aspekte ihrer Informationssicherheitspolitik bestimmen, eine Stakeholderanalyse durchführen und Ziele sowie Richtlinien festlegen. Die Kommunikation dieser Policies und die Zuweisung sowie Kommunikation von Verantwortlichkeiten sind für die erfolgreiche Umsetzung der Sicherheitsstrategien unerlässlich. Das Management von Sicherheitsvorfällen ist ein weiterer kritischer Aspekt, bei dem Organisationen Pläne für das Ansprechen auf und die Behebung von Sicherheitsvorfällen entwickeln müssen. Dies umfasst Abhilfemaßnahmen, Kommunikationspläne und Methoden zur Fortschrittsmessung.

Die zahlreichen Vorgaben und Rahmenwerke bieten die benötigte Hilfestellung für Zulieferer ein sicheres IT-Sicherheitssystem aufzusetzen. Andererseits stellen sie die Zulieferer vor die

Herausforderung die Anforderungen des Gesetzgebers und der OEMs zu verstehen und in ihre existierenden Unternehmensprozesse einzubetten.

Zulieferer müssen bestimmte Prinzipien befolgen, um den wachsenden Anforderungen gerecht zu werden

Durch die steigende Zahl der Software und E/E-Komponenten ergeben sich für die Sicherstellung der IT-Sicherheit einige Prinzipien, die es zu berücksichtigen gilt. Von besonderer Bedeutung ist es, die Prinzipien komplementär zu denken und anzugehen:

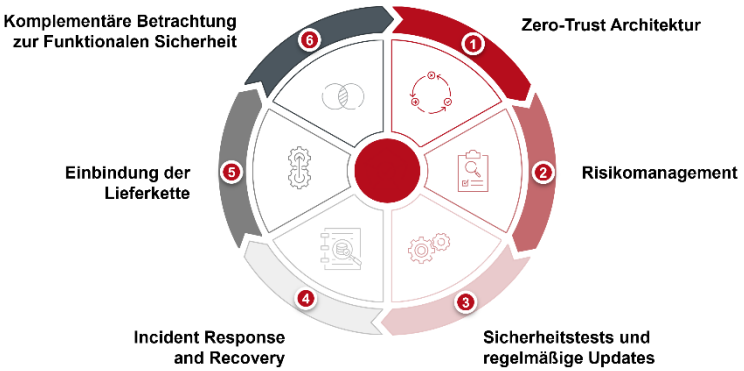

Abbildung 4: Kernprinzipien zur Bewältigung der Anforderungen

1. **Zero-Trust-Architektur:** der Zero-Trust Architektur liegt das Prinzip zu Grunde, niemals blindes Vertrauen zu schenken. Jeder Zugriffsversuch auf das Netzwerk wird sorgfältig geprüft, um sicherzustellen, dass alles sicher und berechtigt ist. Diese Strategie ist besonders wichtig für Zulieferer, da sie hilft, die Angriffsfläche zu verringern und interne Bedrohungen zu minimieren. Eine solide Zero-Trust-Architektur bedeutet, dass Systeme und Daten ständig vor unbefugten Zugriffen geschützt sind.
2. **Risikomanagement:** Risikomanagement ist ein fortwährender und entscheidender Prozess, der den gesamten Lebenszyklus von Fahrzeugkomponenten und -systemen umfasst. Regelmäßige Bewertung und Priorisierung von Sicherheitsrisiken sind unerlässlich, um auf sich wandelnde Bedrohungen adäquat zu reagieren. Hierbei geht es nicht nur um das Erkennen von Risiken, sondern auch um die Entwicklung und Umsetzung von Plänen für den Umgang mit potenziellen Sicherheitsvorfällen, um eine durchgehende Sicherheit zu garantieren.
3. **Sicherheitstests und regelmäßige Updates:** Umfassende Sicherheitstests sind ein Muss für Hersteller und Zulieferer. Dies erfordert Fachwissen in Bereichen wie eingebettete Systeme, IoT, mobile Technologien und Cloud-Systeme. Tests an Schnittstellen zu physischen Komponenten und der Einsatz von automatisierten Tools erhöhen die Qualität der Tests. Außerdem ist es wichtig, Over-The-Air-Updates (OTA-Updates) schnell validieren zu können, um sicherzustellen, dass sie Probleme beheben, ohne neue zu schaffen.
4. **Incident Response und Recovery:** Die Entwicklung und Implementierung von Prozessen für schnelle Reaktionen auf Sicherheitsvorfälle ist unverzichtbar. Diese Maßnahmen ermöglichen eine unmittelbare und wirksame Reaktion, um Schäden zu begrenzen und die Sicherheit rasch wiederherzustellen. Strategien zur Wiederherstellung der

Systemfunktionalität nach einem Angriff sind ebenso entscheidend, um eine schnelle Rückkehr zum Normalbetrieb zu gewährleisten.

5. **Einbindung der Lieferkette:** Eine enge Zusammenarbeit zwischen OEMs und Zulieferern ist entscheidend für die Gewährleistung von Sicherheit. Es ist wichtig, dass alle Beteiligten in der Lieferkette robuste Sicherheitsmaßnahmen implementieren und einhalten. Der regelmäßige Austausch und die gemeinsame Entwicklung von Sicherheitsrichtlinien verstärken die Widerstandsfähigkeit der gesamten Kette.
6. **Komplementäre Betrachtung zur Funktionalen Sicherheit:** IT-Sicherheitsrisiken sollten immer in Verbindung mit der funktionalen Sicherheit eines Fahrzeugs betrachtet werden. Die Einhaltung von Standards wie ISO 26262, ISO/SAE 21434 und ISO 24089 ist entscheidend, um eine umfassende Sicherheit zu gewährleisten. Das bedeutet, dass Safety- und Security-Prozesse Hand in Hand gehen müssen.

Jedes dieser Prinzipien erfordert einen durchdachten Ansatz und eine Strategie, um sicherzustellen, dass die Automobilsoftware sicher und widerstandsfähig gegen verschiedene IT-Sicherheitsbedrohungen ist. Insbesondere müssen Zulieferer ein Konzept entwickeln, wo sie einerseits softwaregeeignete Sicherheitmaßnahmen definieren und andererseits die Interaktion von physischen Komponenten und Software und E/E-Komponenten berücksichtigen, sodass nicht nur eigenständig die Funktionale und IT-Sicherheit sichergestellt wird, sondern eben auch deren Zusammenspiel im Fahrzeug.

Copy with pride - Was die Zulieferer aus der Finanzbranche zur IT-Sicherheit lernen können

In den kommenden Jahren ist mit einer Zunahme regulatorischer Anforderungen für die Automobilindustrie zu rechnen. Dies stellt die Branche vor die anspruchsvolle Herausforderung, kontinuierlich alle Entwicklungen und Neuerungen im Bereich der Regulierung und Compliance im Blick zu behalten und entsprechend umzusetzen. Besonders im Bereich der Informationssicherheit betritt die Automobilindustrie hierbei Neuland, da bisher nur wenig Erfahrung und Expertise in diesem spezifischen Sektor vorhanden ist.

Ein möglicher Ansatz zur Bewältigung dieser Herausforderung könnte sein, sich an anderen Branchen zu orientieren, die bereits über mehr Erfahrung im Umgang mit IT-Risiken und den damit verbundenen regulatorischen Anforderungen verfügen. Ein prägnantes Beispiel hierfür ist die Finanzbranche. Diese stand vor einigen Jahren in Bezug auf die Sicherheit von Kundendaten und die Integrität von Transaktionssystemen vor einer ähnlichen Herausforderung und hat bereits umfangreiche Maßnahmen und Best Practices entwickelt, um diesen Risiken zu begegnen. Hier hat der Gesetzgeber – sowohl auf europäischer als auch nationaler Ebene – in den letzten Jahren Gesetzeslücken in dieser Thematik durch zahlreiche Gesetze und Guidelines geschlossen, wie etwa den EBA-Guidelines zu IKT-Risiken (Guidelines der European Banking Authority zu Informations- und Kommunikationstechnologien), der BAIT (Bankaufsichtliche Anforderungen an die IT) oder der DORA (Digital Operational Resilience Act).

Die Automobilindustrie könnte sich an den Benchmarks und Standards der Finanzbranche orientieren, um effektive und erprobte Strategien zur Risikominderung und zur Einhaltung regulatorischer Vorgaben zu implementieren. Durch den Austausch von Erfahrungen und das Lernen von bewährten Praktiken könnten Automobilhersteller ihre Prozesse optimieren, die

Sicherheit erhöhen und gleichzeitig die Einhaltung der wachsenden regulatorischen Anforderungen sicherstellen. Dies könnte dazu beitragen, das Vertrauen der Kunden zu stärken und die Resilienz der Branche gegenüber Cyberbedrohungen und anderen Sicherheitsrisiken zu erhöhen. Hierbei haben sich verschiedene Vorgehen als besonders geeignet herausgestellt und werden in der Branche mittlerweile als Standard/Benchmark angesehen.

Viele Finanzinstitute haben sich entschieden, sich nach ISO/IEC 27001 zertifizieren zu lassen, damit sie die rechtlichen Anforderungen, wie solche aus der BAIT, erfüllen können. Diese Entscheidung ermöglicht es ihnen, ein umfassendes Informationssicherheitsmanagementsystem zu implementieren, das nicht nur die Sicherheit der Informationstechnologie gewährleistet, sondern auch zur Einhaltung verschiedener regulatorischer Vorgaben beiträgt. Und zwar in einer Weise, sodass mit jeder neuen regulatorischen Anforderung nicht neue Systeme aufgebaut werden müssen, sondern in das existierende IT-Sicherheitssystem integriert werden können. Die ISO/IEC 27001 Zertifizierung bietet so ein solides Fundament für eine systematische Herangehensweise, bei der Sicherheitsrisiken identifiziert, bewertet und durch angemessene Kontrollmechanismen minimiert werden. Durch die Anpassungsfähigkeit der ISO/IEC 27001 können Unternehmen, einschließlich der Automobilzulieferer, aufkommende gesetzliche Rahmenwerke und Sicherheitsstandards effizienter integrieren und umsetzen. Dies fördert nicht nur die kontinuierliche Verbesserung der Informationssicherheit, sondern erleichtert auch die Anpassung an die dynamische Landschaft der regulatorischen Anforderungen in der Automobilindustrie. Anstelle des ISO/IEC 27001 haben Zulieferer auch die Möglichkeit direkt die TISAX-Anforderungen umzusetzen, welches zusätzlich zu den Regelungen im ISO/IEC 27001 auch noch Anforderungen an Datenschutz und Prototypenschutz stellt.

Finanzinstitute nähern sich der Umsetzung von Sicherheitsvorgaben in der Regel durch eine strategische Planung, was mit der Aufstellung einer IT-Strategie bzw. Ergänzung der bestehenden Strategie und dem Aufsetzen von entsprechenden Dokumenten und Strukturen einhergeht. Ein übergreifendes Framework stellt sicher, dass alle Sicherheitsmaßnahmen und -prozesse mit den Geschäftszielen und der Risikotoleranz der Organisation in Einklang stehen und ermöglicht eine längerfristige Planung, nicht nur eine standardabhängige Umsetzung. Es ermöglicht zudem, Ressourcen effizienter zu nutzen, indem es Redundanzen eliminiert und sicherstellt, dass Sicherheitsmaßnahmen und -prozesse aufeinander abgestimmt sind.

Im ISO/IEC Standard 21434 sind bereits spezifische Richtlinien für das Drittanbietermanagement im Bereich der Cybersicherheit in der Automobilindustrie festgelegt. Ein zentraler Aspekt dabei ist die Verwaltung von verteilten Cybersicherheitsaktivitäten. Kernelement sind hier die Evaluierung der Fähigkeiten der Lieferanten, Cybersecurity Interface Agreements und die Aufstellung einer Responsibility Assignment Matrix. In der ISO/IEC 27001 finden sich ähnliche Anforderungen, welche die Finanzbranche umgesetzt hat. Ein wesentlicher Aspekt hierbei ist die Verlagerung der Verantwortungen (soweit zulässig) auf die Drittanbieter, also ähnlich wie OEMs auch bestimmte Pflichten auf Zulieferer übertragen. Für Zulieferer empfiehlt sich demzufolge wie möglich die Pflichten an ihre Zulieferer weiterzugeben. Hierfür sind sowohl standfeste Vertragsklauseln in die Lieferantenverträge aufzunehmen, als auch Prozesse für regelmäßige

Audits aufzusetzen. Dies erlaubt Zulieferern zumindest ein Teil der Verantwortung abzugeben, und über die Lieferkette hinweg bereits die Sicherheitsstandards festzulegen.

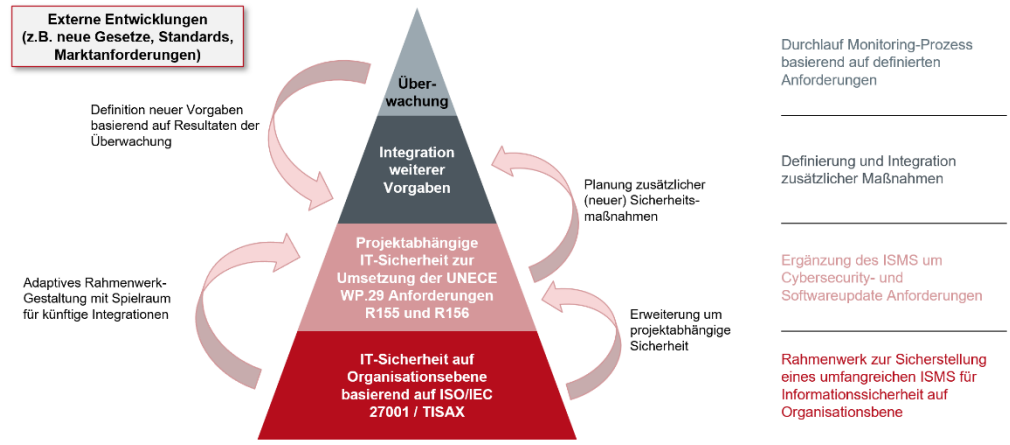

Abbildung 5: Überblick über strategische Konzeption eines IT-Sicherheitsmanagementsystems

Allgemein lässt sich aus der Finanzbranche ableiten, dass ein systematischer und strukturierter Ansatz für die langfristige Gewährleistung der Erfüllung der Sicherheitsvorgaben auf verschiedenen Ebenen – der IT-Sicherheit, dem Datenschutz, der Cybersicherheit, der funktionalen Sicherheit und den Software-Updates zielführend sind. Anstelle zahlreicher parallel laufender Systeme erlaubt diese Vorgehensweise, dass die einzelnen Bausteine aufeinander aufbauen, wodurch Effizienz und Adaptibilität geschaffen werden. Als Grundbaustein dient hierbei die Erfüllung der Mindestanforderungen an die interne Unternehmenssicherheit und weitergehend die vollumfängliche Umsetzung der Vorgaben aus dem ISO/IEC 27001/TISAX. Darauf aufbauend lässt sich das System, um die automobilspezifischen Standards zu CSMS und SUMS erweitern, welche dann einerseits auf Projektebene, andererseits für die externe Umgebung also die Fahrer und Verkehrsteilnehmer die Sicherheit garantiert. Als dritter Baustein wird gewährleistet, dass das bestehende System die Integration weiterer Vorgaben ohne eine wesentliche und überflüssige Komplizierung der bestehenden Maßnahmen und Prozesse vollziehen kann. Schließlich ist als Sicherheitkontrolle „on top“ hier dann ein umfassendes Monitoring aufgesetzt, welches die Effektivität und Vollständigkeit der bestehenden Maßnahmen überwacht und erlaubt Schwachstellen ressourcensparend zu identifizieren und eliminieren.

Eine Vereinbarung von verschiedenen -Sicherheitskonzepten erlaubt effizientes Management der zahlreichen Anforderungen

Die Harmonisierung von Hardware- und Software-Sicherheitskonzepten spielt eine entscheidende Rolle in der Automobilindustrie. Dies kann durch die parallele Betrachtung der Safety- und Security-Anforderungen und den daraus abgeleiteten Prozessen verwirklicht werden.

Ein zentraler Aspekt hierbei ist das Safety Engineering, das sich auf den systematischen Prozess konzentriert, um die Sicherheit eines Fahrzeugs während seines gesamten Lebenszyklus zu gewährleisten. Es beinhaltet die Identifizierung, Bewertung und Minderung von Risiken, die mit der Funktionsweise eines Fahrzeugs verbunden sind, insbesondere in Bezug auf die physische Sicherheit der Insassen und anderer Verkehrsteilnehmer. Schlüsselbereiche wie funktionale Sicherheit, Fahrzeugsicherheit, IT-Sicherheit, Umweltsicherheit und Notfallreaktionen sind hierbei von großer Bedeutung.

Die Synchronisation von Produktion, Entwicklung und Testen ist ein weiterer wichtiger Pfeiler im Sicherheitsmanagement. Sicherheitstests sollten nicht als isolierte Phase betrachtet werden, sondern als integraler Bestandteil des Entwicklungsprozesses von Anfang an. Dies bedeutet, dass Sicherheitstests parallel zur Softwareentwicklung und Fahrzeugproduktion durchgeführt werden sollten, um Schwachstellen frühzeitig zu erkennen und zu beheben. Dieser Ansatz minimiert nicht nur die Kosten für spätere Fehlerbehebungen, sondern fördert auch eine Kultur der Qualität und Sicherheit in allen Stufen der Fahrzeugentwicklung. Zusätzlich ist die Überprüfung der Softwarezusammensetzung, insbesondere der verwendeten Open-Source-Komponenten entscheidend, um bekannte Schwachstellen zu identifizieren. Dies ist ein wesentlicher Schritt, um die Sicherheit der Automobilsoftware zu gewährleisten. Ein besonderes Augenmerk sollte auf Integrationstests gelegt werden. Da viele Automobilsoftwarekomponenten von verschiedenen Teams entwickelt werden ist es wichtig, die Integration aller Komponenten sorgfältig zu testen. Insbesondere die der Hardware und Software. Dies stellt eine nahtlose Zusammenarbeit aller Systeme sicher und gewährleistet, dass keine Sicherheitslücken entstehen.

Durch die Schaffung einer einheitlichen Sicherheitsstrategie, die sowohl physische Komponenten als auch digitale Systeme aus einer Safety und Security-Perspektive betrachtet, können Zulieferer die Komplexität der verschiedenen Anforderungen effektiver bewältigen. Eine solche integrierte Vorgehensweise ermöglicht es, Sicherheitsrisiken systematisch zu identifizieren und zu mindern, wodurch die Einhaltung branchenspezifischer Standards erleichtert wird. Für Automobilhersteller und Zulieferer resultiert dies in einer verbesserten Produktqualität und einem stärkeren Vertrauen der Endkunden in die Fahrzeugsicherheit.

Weiterhin ist es wichtig, dass die Sicherheitsstrategie dynamisch und anpassungsfähig bleibt, um auf neue Bedrohungen und technologische Entwicklungen reagieren zu können. In der schnelllebigen Welt der Automobiltechnik, wo ständig neue Software-Updates und Hardware-Verbesserungen eingeführt werden, muss die Sicherheitsstrategie flexibel genug sein, um diese Änderungen zu integrieren, ohne die grundlegende Sicherheitsintegrität zu beeinträchtigen.

Die enge Zusammenarbeit zwischen Automobilherstellern, Zulieferern und Sicherheitsexperten ermöglicht einen kontinuierlichen Informationsaustausch über potenzielle Sicherheitslücken und deren Behebung. Durch regelmäßige Sicherheitsaudits und -bewertungen können Schwachstellen frühzeitig erkannt und behoben werden, was zu einer stetigen Verbesserung der Sicherheitsstandards führt.

Fazit

In der Automobilbranche sind bereits zahlreiche Sicherheitsmaßnahmen implementiert worden, darunter Zertifizierungen nach Standards wie TISAX oder ISO/IEC 27001. Doch um den wachsenden Herausforderungen und Erwartungen in Bezug auf Software-Sicherheit gerecht zu werden, ist eine kontinuierliche und umfassende Bestandsaufnahme unerlässlich. Dies gilt insbesondere für Zulieferer, die eine Schlüsselrolle in der Entwicklung und Bereitstellung sicherer Automobilkomponenten spielen. Durch die Identifizierung von Schwachstellen und das Erschließen von Optimierungspotenzialen können Zulieferer sicherstellen, dass ihre Produkte den höchsten Sicherheitsstandards entsprechen.

Für die Zukunft ist es entscheidend, eine zukunftsgerichtete Strategie zu entwickeln, die ein klares Zielbild umfasst und neue Prozesse einführt. Zulieferer können dabei von Branchen wie der Finanzbranche lernen, die bereits fortschrittliche Sicherheitsstandards und Compliance-Maßnahmen etabliert haben. Ein solcher Ansatz ermöglicht es den Zulieferern, nicht nur aktuellen Anforderungen gerecht zu werden, sondern auch proaktiv auf zukünftige regulatorische Entwicklungen zu reagieren.

Die Integration von künstlicher Intelligenz und maschinellem Lernen in die Sicherheitskonzepte bietet eine hervorragende Möglichkeit, ungewöhnliche Muster oder Anomalien zu erkennen, die auf potenzielle Sicherheitsbedrohungen hinweisen könnten. Dieser innovative Ansatz kann die Effektivität der Sicherheitsmaßnahmen erheblich steigern, indem er ihnen hilft, Risiken frühzeitig zu identifizieren und zu mitigieren.

Die Einbeziehung der Perspektive der Endkunden in die Sicherheitsstrategie ist ebenfalls ein wichtiger Aspekt. Zulieferer können durch die Bereitstellung von Informationen über die Sicherheitsfeatures ihrer Komponenten dazu beitragen, das Bewusstsein und die Verantwortung der Fahrer für die Fahrzeugsicherheit zu stärken. Dies trägt nicht nur zur Sicherheit des einzelnen Fahrers bei, sondern erhöht auch die allgemeine Verkehrssicherheit.

Zusammenfassend lässt sich sagen, dass eine umfassende und dynamische Sicherheitsstrategie, die Hardware, Software und menschliche Faktoren integriert, essentiell ist, um eine robuste Verteidigung gegen Sicherheitsbedrohungen zu gewährleisten. Dies stellt sicher, dass sie den sich ständig ändernden Anforderungen an Sicherheit und Zuverlässigkeit gerecht werden und das Vertrauen der Kunden stärken.

Abbildungsverzeichnis

Quellen

https://www.adac.de/rund-ums-fahrzeug/ausstattung-technik-zubehoer/autonomes-fahren/recht/autonomes-fahren-hacker-angriff/

https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/mapping-the-automotive-software-and-electronics-landscape-through-2030

https://upstream.auto/reports/global-automotive-cybersecurity-report/

https://www.faz.net/aktuell/wirtschaft/unternehmen/autohersteller-und-zulieferer-verbunden-auf-gedeih-und-verderb-14402472.html

https://www.lv.com/insurance/press/keyless-technology-drives-rise-in-theft-over-past-four-years

Fabian Meyer leitet als Managing Partner COREconsulting mit dem Schwerpunkt auf Internationalisierung der CORE-Angebote. In der Klientendimension verantwortet er die Umsetzung komplexer IT-Projekte mit Schwerpunkten auf Merger & Akquisitions, Payments und Transaction Banking. Bereits während seines betriebswirtschaftlichen Studiums, das er mit einem Mastergrad in Mannheim abschloss, konnte er Erfahrungen als Unternehmensberater und -gründer sammeln. Er verfügt über mehrjährige Beratungserfahrung im Technologiesektor.

Mail: fabian.meyer@core.se

Marian Matthies ist Senior Transformation Manager bei CORE und verfügt über mehrere Jahre Erfahrung in der Automobilbranche. Sein profundes Branchenwissen basiert dabei sowohl auf operativer Tätigkeit, als auch der Leitung von strategischen, groß angelegten Transformationsprojekten in verschiedenen Bereichen des Verticals. Bei CORE verantwortet er zudem die Leitung des Kompetenzbereichs Automotive.

Mail: marian.matthies@core.se

Muskaan Multani ist Transformation Fellow bei CORE und hat einen Hintergrund im Wirtschaftsrecht und in der strategischen Beratung. Als Legal Consultant sowie durch diverse Praktika während ihrer Studienzeit hat sie bereits diverse Projekte im Compliance-Bereich begleitet. Sie ist verantwortlich für die Unterstützung von Projektteams und Kunden bei geschäftskritischen Technologietransformationen.

Mail: muskaan.multani@core.se

COREtransform GmbH
Kurfürstendamm 194
10707 Berlin | Deutschland
https://core.se/
Telefon: +49 30 263 440 20
office@core.se

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
https://core.se/
Telefon: +41 44 261 0143
office@core.se

COREtransform Ltd.
9 Devonshire Square, 5th Floor
London EC2 4YF
Großbritannien
https://core.se/
Telefon: +44 20 328 563 61
office@core.se

COREtransform Consulting MEA Ltd.
DIFC – 105, Currency
House, Tower 1
P.O. Box 506656
Dubai I Vereinigte Arabische Emirate
https://core.se/
Telefon: +97 14 323 0633
office@core.se