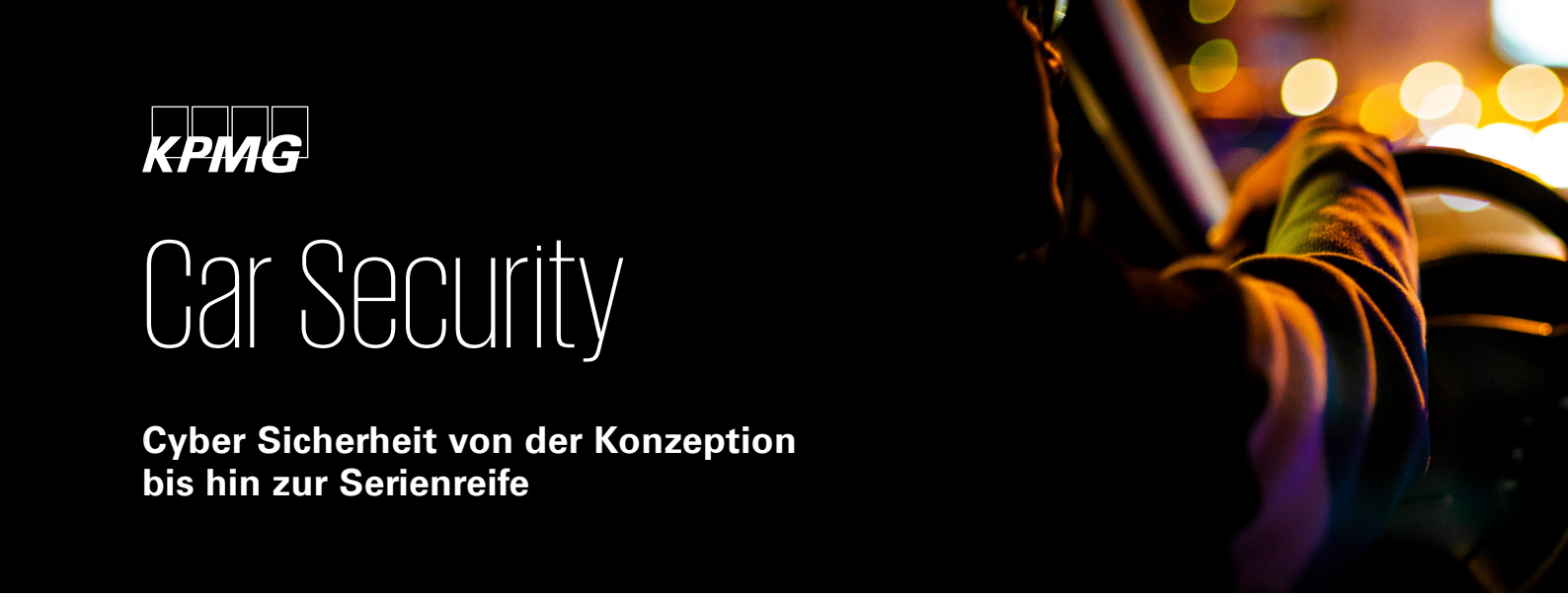

Car Security

Cyber Sicherheit von der Konzeption bis hin zur Serienreife

Die Automobilindustrie gerät durch steigende Digitalisierung und Vernetzung der Fahrzeuge immer mehr in das Visier von Cyber-Angreifern. Aus diesem Grund setzt die UNECE ab 2022 ein Cyber-Security-Managementsystem für die Typenzulassung voraus.

Die Herausforderung

Mittlerweile werden fortlaufend Angriffe bekannt, die sich insbesondere die zunehmenden Software-Anteile und Vernetzung der Fahrzeuge zunutze machen. Der weitere Anstieg von Software und Kommunikation wird das Risiko von Cyber-Angriffen massiv erhöhen und sowohl das zukünftige Geschäftsmodell der Mobilitätsdienstleister als auch Leib und Leben der Verkehrsteilnehmer bedrohen. Dies führt dazu, dass in den nächsten Jahren Software und deren Verlässlichkeit zum Verkaufsargument und Alleinstellungsmerkmal von Automobilherstellern und ebenso deren Zulieferern werden wird.

Dies hat auch der Regulator erkannt. Das Weltforum für die Harmonisierung von Fahrzeugvorschriften der Vereinten Nationen (WP.29) entwickelt derzeit eine Regulierung, die Cyber Security relevant für die Zulassung neuer Fahrzeugtypen macht. Der Vorschlag der Unterarbeitsgruppe TF-CS/OTA besteht aus zwei Kernforderungen: die Implementierung und der Betrieb eines zertifizierten Cyber-Security-Managementsystems (CSMS) sowie die Anwendung des CSMS auf den konkreten Fahrzeugtyp zum Zeitpunkt der Typzulassung. Diese Entwicklungen zeigen: Cyber Security wird zum kritischen Erfolgsfaktor in der Automobilindustrie und gehört auf die CEO-Agenda.

Mit der UN-Regulierung wird Cyber Security über den unverbindlichen Status hinauswachsen und zu einer Voraussetzung für die Geschäfts- und Wettbewerbsfähigkeit von Herstellern und Zulieferern werden. Dies spiegelt auch die Kundensicht wider. Nach einer aktuellen Studie[(a)] bilden Cyber Security und Datenschutz aus Kundensicht die wichtigsten Kaufkriterien und eine Grundvoraussetzung für den Kauf eines Fahrzeuges, analog etwa zu einem Anschnallgurt oder Airbag. Im Kontext des digitalen Wandels gilt es dementsprechend, nicht nur die Regulierung zu erfüllen, sondern bezogen auf die jeweilige Unternehmensstrategie und Produkt-Roadmap den optimalen Ansatz mit der höchsten Wirksamkeit zu finden.

Die Unternehmen müssen dementsprechend ganzheitlich organisatorische und technische Maßnahmen implementieren, die es ermöglichen, Cyber Security in der gesamten Wertschöpfungskette dauerhaft zu definieren, zu kontrollieren, zu steuern und zu verbessern.

Eine schnelle, risikobasierte und konforme Umsetzung der „Produktperspektive Cyber Security" wird dadurch zum zentralen Aspekt der Wettbewerbsfähigkeit von Herstellern und Zulieferern, um eine reibungslose Typenzulassung garantieren zu können. Voraussetzung hierfür ist ein zertifiziertes CSMS.

Die Zeit drängt, denn die UNECE plant die Umsetzung der Regulierung bis 2022 für neue Fahrzeuge und bis 2024 für alle Fahrzeugtypen einzuführen.

Unsere Leistung – Ihr Nutzen

Wir können Sie von der ersten Fit-Gap-Analyse über die Implementierung eines zertifizierungsfähigen CSMS bis hin zur Typzulassung begleiten. Gemeinsam mit unserem Kooperationspartner ESCRYPT haben wir hierfür das Framework PROOF entwickelt.

Im ersten Schritt kann ein Readiness Assessment Ihrem Unternehmen einen Überblick über Verbesserungspotenziale und Gaps bezüglich der aufkommenden Regulierungen verschaffen, sowie aufzeigen, in welchen Handlungsfeldern Ihr Unternehmen bereits gut aufgestellt ist.

Anm.: (a) siehe Global Automotive Survey 2020, KPMG

Auf Basis dieser Ergebnisse entsteht ein vollumfängliches Bild davon, was zu der Erreichung des Zertifikats umzusetzen ist, um weiterhin problemlos eine Typenzulassung für neu entwickelte Fahrzeuge und ab 2024 für bereits bestehende Fahrzeuge zu erhalten.

PROOF – Unser CSMS Framework

Von Readiness Checks über die Entwicklung als auch Implementierung eines CSMS bis hin zu einer risikoadäquater Fahrzeugsicherheit bieten wir Ihrem Unternehmen unser erprobtes Framework an, um die Anforderungen konform umzusetzen. Das Framework basiert auf den einschlägigen Standards ISO 21434 (Entwurf) und ISO 24089 (Entwurf) und wird durch unsere langjährige Beratungs- und Prüfungserfahrung in den Bereichen Cyber Security Governance, Management-Systeme und Risikomanagement ergänzt. Es besteht aus den fünf übergeordneten Domänen:

- Cyber Security Governance
- Risk Management
- Concept & Development
- Production & Operations
- Ecosystem

Diese können je nach Bedarf flexibel eingesetzt werden.

Bestens für Sie aufgestellt

Unsere Kooperation mit ESCRYPT bietet die Möglichkeit, die Stärken beider Unternehmen gemeinsam zu nutzen, um sowohl Fahrzeughersteller als auch deren Zulieferer dabei zu unterstützen, kritischen Businessanforderungen an Cyber Security effizient nachzukommen. Dabei hat KPMG jahrelange Erfahrung in den Bereichen Entwicklung und Implementierung von Management-Systemen, sowie die Überwachung von Informationssicherheits-Management-Systemen. ESCRYPT zeichnet sich insbesondere durch die jahrelange Erfahrung im Bereich Car Security und die Kenntnis über alle relevanten Standards und Vorgaben für ein CSMS und SUMS aus.

Darüber hinaus verfügen KPMG und ESCRYPT über ein breites Netzwerk von mehr als 300 Expertinnen und Experten in ganz Deutschland zu unterschiedlichen Cyber-Security-Themenstellungen, um auf sich ändernde Anforderungen schnell reagieren zu können.

Gemeinsam verfügen wir über die nötige technische Erfahrung, als auch die organisatorische Tiefe, um Cyber Security effizient und global zu implementieren und auszurollen.

Sie haben Fragen? Sprechen Sie uns gerne an.

PROOF – Unser CSMS Framework

Kontakt

KPMG AG
Wirtschaftsprüfungsgesellschaft

Klingelhöferstraße 18
10785 Berlin

Hans-Peter Fischer
Partner, Cyber Security
T +49 69 9587-2404
hpfischer@kpmg.com

Andrzej Wozniczka
Senior Manager, Cyber Security
T +49 211 475-7516
awozniczka@kpmg.com

Jan Stölting
Senior Manager, Cyber Security
T +49 69 9587-6273
jstoelting@kpmg.com

www.kpmg.de

www.kpmg.de/socialmedia