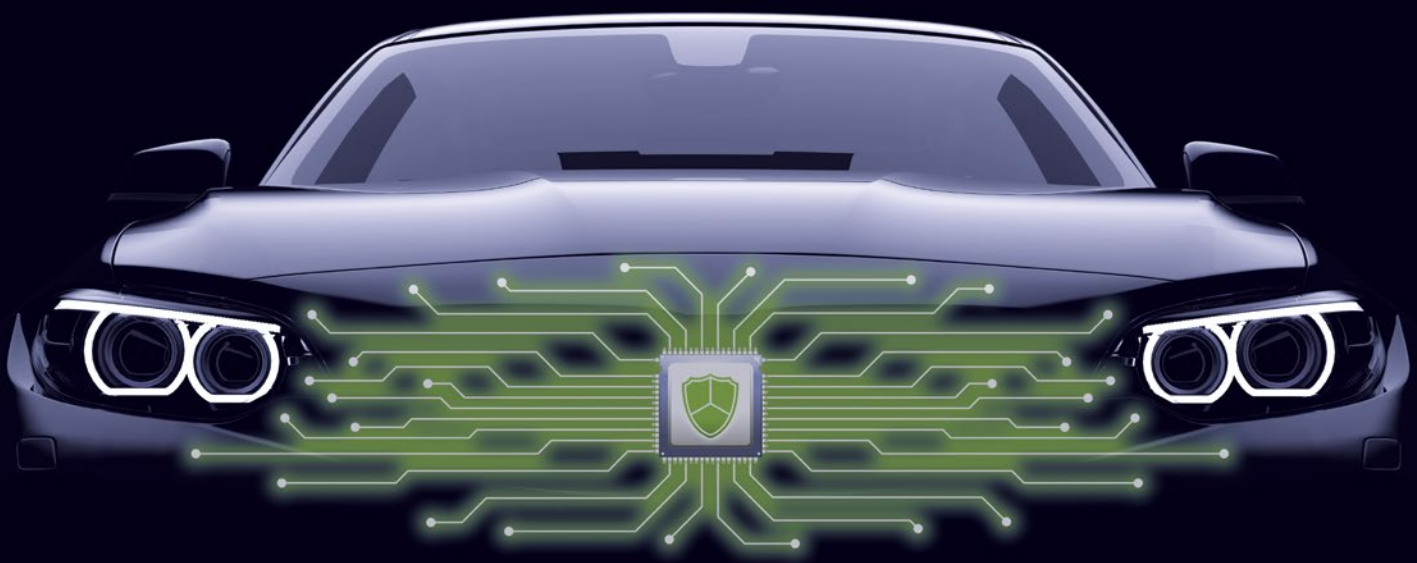
escrypt
SECURITY. TRUST. SUCCESS.

in Kooperation mit
KPMG

Whitepaper

Wie Digitalisierung und Automatisierung Automobilhersteller wie -zulieferer vor neue Security-Herausforderungen stellt.

Cybersicherheit in voller Fahrt



Als Carl Benz 1886 das Automobil präsentierte, hatte er sicherlich mit anderen Sicherheitslücken zu kämpfen als heutige Autohersteller. Von mechanischer Sicherheit über die Erfindung des Sitzgurtes hat die Entwicklung des Automobils über 100 Jahre zurückgelegt, bis Cybersicherheit relevant wurde. Seitdem haben diverse Cyberangriffe auf Autos das Thema in den Fokus der Öffentlichkeit und auch des Gesetzgebers gebracht. Eine Arbeitsgruppe der Vereinten Nationen entwickelt nun eine Regulierung, welche für die gesamte Branche einen Paradigmenwechsel bedeutet: Die Typzulassung von Fahrzeugen wird künftig nur noch mit der Zertifizierung eines Cybersecurity-Managementsystems (CSMS) möglich sein. Damit muss Cybersicherheit auf der Agenda eines jeden Automobil-CEOs stehen.

Inhalt

Evolution der automobilen Cybersicherheit

Einen der ersten Hacks eines Automobils, der veröffentlicht wurde, machten 2009 eine Gruppe von Wissenschaftlern um Stephen Checkoway. Sie beschrieben, wie sie einen Laptop an einen Kontrollzugang des Autos anschlossen, um auf das interne Netzwerk des Fahrzeugs zuzugreifen. Dadurch waren sie in der Lage, kritische Systeme des Autos zu manipulieren. So konnten sie beispielsweise den Motor abschalten oder die Bremsen blockieren. Bei dem Angriff nutzten die Wissenschaftler diverse Schwachstellen des Fahrzeugnetzwerks und der Steuergeräte aus, um manipulierte Datensätze an die eingebetteten Systeme des Autos zu senden und deren Funktionen zu beeinflussen. Zwar dürfte es für Angreifer schwer sein, einen Laptop an das Fahrzeug ihrer Opfer anzuschließen, aber auch kleinere, ferngesteuerte Geräte wären in der Lage, diesen Schaden anzurichten und damit die Sicherheit der Verkehrsteilnehmer zu bedrohen.

Im Jahr 2010 schaffte es ein 20-jähriger, über 100 Autos ferngesteuert zu manipulieren, sodass diese nicht mehr starteten. Der Vermieter „Texas Auto Center" hatte in seinen Mietwägen Hardware verbaut, die über ein Online-System angesprochen werden konnte. Mit diesem System konnte der Vermieter die Zündung deaktivieren, sollte der Mieter nicht zahlen. Der Hacker war kurz zuvor entlassen worden und verschaffte sich nun über ein Mitarbeiterkonto Zugang zum System. Er erlangte anschließend Kontrolle über die entsprechenden Hardware-Komponenten der Mietwagenflotte.

Noch kritischer wurde es 2015, als Charlie Miller und Chris Valasek es schafften, einen Jeep ferngesteuert zu übernehmen. Über das Entertainment-System des Geländewagens erlangten sie Zugriff auf Multimediasysteme, Scheibenwischer, Klimaanlage, Bremsen und die Geschwindigkeit des Fahrzeugs. Sie stoppten das Auto, dessen Fahrer als Tester angeheuert war, mitten auf der Autobahn. Dazu mussten sie sich nicht wie im Artikel von 2009 per Kabel mit dem Auto verbinden, sondern sie nutzten die Internetverbindung des Wagens. Chrysler musste im Anschluss circa 1,4 Millionen Fahrzeuge zurückrufen und ausbessern.

Mittlerweile werden fortlaufend Angriffe bekannt, die sich insbesondere die zunehmende Digitalisierung und Vernetzung der Fahrzeuge zunutze machen. Im Licht dieser Entwicklung wird ersichtlich, welches Risiko nicht ausreichend geschützte Fahrzeuge für Hersteller, Besitzer und Verkehrsteilnehmer bergen. Mit der zunehmenden Anzahl und Komplexität der in Autos verbauten IT-Systeme steigen daher auch die Anforderungen an Cybersicherheit. Das Fahrzeug als abgeschlossenes System zu betrachten, steht im direkten Widerspruch zu einem angemessenen, risiko-basierten Sicherheitsansatz. Neue digitale (Online-) Dienste, die im Auto zur Verfügung stehen, die Kommunikation zwischen Fahrzeugen und Herstellern (Over the Air Updates), die Fahrzeug-zu-Fahrzeug-Kommunikation (Car 2 Car) und die Kommunikation zwischen Auto und Infrastruktur (Car 2 Infrastructure) sowie mit Smartphones und Geräten von Drittanbietern bieten enorme Angriffsflächen, die systematisch betrachtet und beherrscht werden müssen. ■

Neue Vorgaben für die Cybersicherheit von Fahrzeugen

Weltweit laufen Aktivitäten um Cybersicherheit weiter zu regulieren und zu standardisieren. Es gibt Gesetzesvorschläge im US-Kongress, den Cybersecurity Act in der EU, das chinesische ICV-Programm und neue Guidelines von JASPAR in Japan. In allen lassen sich drei wesentliche Trends erkennen: Eine stärkere Konkretisierung von Cybersicherheit auf Spezifika der Automobilindustrie, die Herausforderung und Anforderung die Sicherheit im Feld aufrecht zu erhalten, sowie der immer häufigere verpflichtende Charakter der Vorgaben und deren Überprüfung zum Zeitpunkt der Typzulassung. Diese Trends spiegeln sich insbesondere in der UNECE WP.29 TF-CS/OTA und der ISO/SAE 21434, die explizite Managementsysteme zum Schutz von Fahrzeugen definieren.

UNECE WP.29 TF-CS/OTA

Das Weltforum für die Harmonisierung von Fahrzeugvorschriften der Vereinten Nationen (WP.29) hat im Juni 2020 eine Regulierung verabschiedet, die Cybersicherheit relevant für die Zulassung neuer Fahrzeugtypen macht. Der Vorschlag der Unterarbeitsgruppe TF-CS/OTA besteht aus zwei Kernforderungen: Dem Betrieb eines zertifizierten Cybersecurity-Managementsystems (CSMS) sowie der Anwendung des CSMS auf den konkreten Fahrzeugtyp zum Zeitpunkt der Typzulassung. Die EU plant, die Einhaltung dieser Vorgaben bereits ab dem ersten Halbjahr 2022 einzufordern.

In Anbetracht typischer Entwicklungszeiten im Automobilbereich müssen sich Hersteller und Zulieferer also bereits heute mit diesen Cybersicherheits-Anforderungen auseinandersetzen, um die Typzulassungen für ihre nächsten Produkte sicherstellen zu können. Dazu müssen sie einen risikobasierten Ansatz verfolgen, der durchgängig für den Fahrzeugtyp, dessen externen Schnittstellen und dessen Subsysteme ein angemessenes Risikoniveau ermitteln, erreichen und erhalten kann. Dies schließt insbesondere die Berücksichtigung von Abhängigkeiten und Informationen von Zulieferern, Dienstleistern und weiteren Dritten aus Sicht der Cybersicherheit ein.

Im Angesicht des sich stetig wandelnden Bedrohungsumfelds und der langen Fahrzeuglebenszyklen liegt ein wesentlicher Fokus des geforderten CSMS auf der Phase nach Produktionsstart und der kontinuierlichen Risikobehandlung im Fahrzeugbetrieb. Somit erhält das Thema des prozessual organisierten Sicherheitsmanagements regulatorisch auch in der Automobilindustrie Einzug. Während auf Erfahrung mit Informationssicherheitsstandards wie der ISO 27000-Reihe zurückgegriffen werden kann, liegt die wesentliche Herausforderung bei der Ausgestaltung eines CSMS in der Berücksichtigung der Automobilspezifika. Neben der hohen Komplexität sowohl des Produkts als auch der Lieferkette stellen vor allem Wechselwirkungen mit der funktionalen Sicherheit, die Einhaltung von Umweltvorschriften und der Diebstahlschutz kritische Aspekte dar.

ISO/SAE 21434

Parallel zur TF-CS/OTA erarbeitet die Automobilindustrie im Kontext der Internationalen Organisation für Standardisierung (ISO) und dem Verband der Automobilingenieure (SAE) den Standard ISO/SAE 21434 für Cybersicherheit von Fahrzeugen. Analog zum durch die WP.29 definierten CSMS legt diese Norm den Fokus auf die richtige Organisation und die richtigen Prozesse entlang des kompletten Lebenszyklus von Fahrzeugen, um diese vor Cyberattacken zu schützen. Da ein Begleitdokument des UN-Regulierungsentwurfs konsequent auf diesen Standard zur Umsetzung der CSMS-Anforderungen verweist, verdient die ISO/SAE 21434 besondere Aufmerksamkeit. Mit einer gemeinsamen Terminologie und definierten Maßnahmen wird eine industrieweite Grundlage geschaffen, auf der Hersteller und Zulieferer ihre Schnittstellen, geteilten Verantwortlichkeiten und Prozesse aufbauen können. Die finale Fassung wird Ende 2020 erwartet. ■

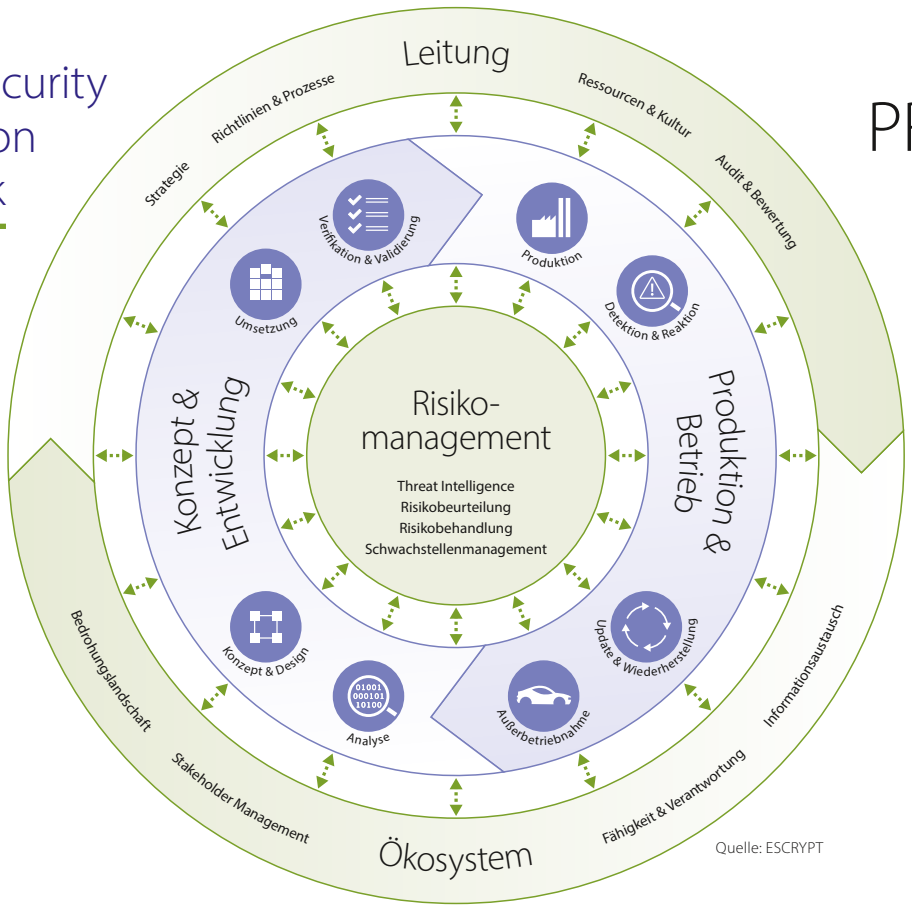
Auswirkungen auf die Automobilindustrie

Die Automobilindustrie wird bereits länger vom Gesetzgeber reguliert. Gesetzliche Vorgaben zur Informations- oder Cybersicherheit kennt diese Branche allerdings nur vereinzelt. Aufgrund des wachsenden Bedarfs der OEMs an Transparenz über das Informationssicherheitsniveau der Zulieferer hat der Verband der Automobilindustrie (VDA) einen Katalog für Information Security Assessments (ISA) entwickelt. Mit dem TISAX-Modell (Trusted Information Security Assessment Exchange) steht OEMs ein Mechanismus zur Verfügung, anhand des Katalogs den Umgang der Zulieferer mit sensiblen Daten, beispielsweise im Kontext von Prototypen, zu überprüfen.

Neben TISAX setzt nun die ISO/SAE 21434 Anforderungen an die Cyber- und Produktsicherheit. Spätestens seit dem Jeep-Hack 2015 hat die Automobilindustrie den Schutz von Fahrzeugen verstärkt. Mit der UN-Regulierung wird Cybersicherheit jedoch über den unverbindlichen Status hinauswachsen und zu einer Voraussetzung für die Geschäfts- und Wettbewerbsfähigkeit von Herstellern und Zulieferern werden. Im Kontext des digitalen Wandels gilt es 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, Cybersicherheit in der gesamten Wertschöpfungskette dauerhaft zu definieren, zu kontrollieren, zu steuern und zu verbessern. Konsequenterweise wächst bereits heute der Bedarf an so genannten Lückenanalysen, die den Stand der Umsetzung eines CSMS ermitteln und daraus gezielte Verbesserungsfahrpläne ableiten. ■

Product Security Organization Framework

PROOF



Quelle: ESCRYPT

Fachkundige Unterstützung

Wie viele andere Branchen wird auch die Automobilindustrie auf einen Fachkräftemangel blicken: Experten, die sowohl Cybersicherheit als auch die speziellen Anforderungen der Automobilindustrie verstehen sind rar. Gleichzeitig wachsen die Cyberrisiken aufgrund der Digitalisierung so rasant, dass das eigene Wissen der Unternehmen auf dem Gebiet der Cybersicherheit typischerweise nicht ausreicht, um alle Herausforderungen rechtzeitig allein zu bewältigen. Denn aufgrund der Typzulassungsrelevanz ist es kritisch, bereits im ersten Anlauf alle Anforderungen sicher und möglichst effizient umzusetzen.

Kooperation ESCRYPT und KPMG

An dieser Stelle bieten die Beratungsunternehmen ESCRYPT und KPMG passende Dienstleistungen an, um Hersteller wie Zulieferer erfolgreich durch die Entwicklung konformer Sicherheitslösungen zu leiten. ESCRYPT hat langjährige Erfahrung darin, Cybersicherheit in der Automobilindustrie von der Konzeption bis hin zur Serienreife zu führen und anschließend im Betrieb das gewünschte Sicherheitsniveau aufrechtzuerhalten. KPMG ist Experte in Informationssicherheit und dem Assessment und Ausrollen von Sicherheitsmanagementsystemen. Die enge Verzahnung dieser Stärken in der Kooperation ermöglicht einen holistischen Ansatz, der den Nutzen für Kunden erhöht. So können notwendige Änderungen auf der Organisations- und Prozessebene derart gestaltet werden, dass die Auswirkungen auf die Entwicklung und den Betrieb der Sicherheitslösungen berücksichtigt und optimiert sind.

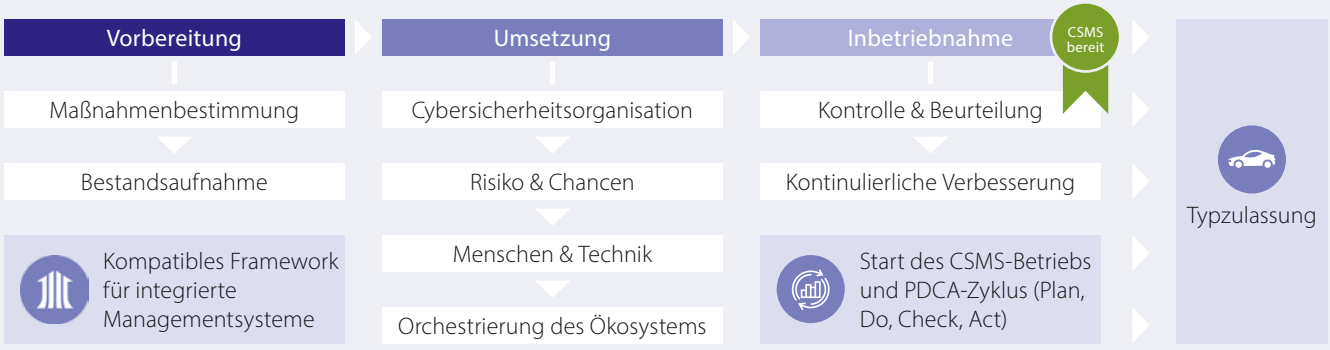
Bewährte Vorgehensweise

ESCRYPT und KPMG unterstützen die Automobilindustrie in allen relevanten Märkten und Nischen, von Herstellern von Luxussportwagen bis zu den globalen Top 5 OEMs und führenden Zulieferern für hochautomatisiertes Fahren. Die Dienstleistungen folgen einer bewährten Vorgehensweise, die auf der jahrzehntelangen Erfahrung der Kooperationspartner beruht: Sie führt in drei Schritten von der Vorbereitung über die Umsetzung zur Inbetriebnahme und kontinuierlichen Verbesserung.

Mit eigenen Stärken schneller zum Ziel

Im Angesicht der Komplexität der Gesamtherausforderung der Digitalisierung sowie dem bald erforderlichen Nachweis von Cybersicherheit bei Typzulassung ist es unerlässlich, soweit möglich eigene vorhandene Stärken zu identifizieren, gezielt weiterzuentwickeln und zu einem ganzheitlichen Cybersicherheit-Managementsystem zusammenzufügen. Das können beispielsweise bestehende Informationssicherheits-Managementsysteme (ISMS), Qualitäts-Managementsysteme oder etablierte Praktiken zur Erreichung funktionaler Sicherheit sein. An dieser Stelle bieten ESCRYPT und KPMG spezialisierte Audits und Fit/Gap-Analysen, die sowohl potenzielle Lücken zu relevanten Standards ermitteln als auch vorhandene Stärken aufdecken und so ein Benchmarking und eine Priorisierung von Maßnahmen ermöglichen, die den Return-on-Investment maximieren sollen und möglichst schnell zum Ziel führen. ■

Bewährte und strukturierte Methodik für die Einführung eines CSMS



Quelle: ESCRYPT

Kontakt

Dr. Moritz Minzlaff
Senior Manager
moritz.minzlaff@escrypt.com
Telefon +49 30 40369-1901

Dr. Martin Emele
Vice President Cybersecurity
martin.emele@etas.com
Telefon +49 711 3423-3054

ESCRYPT GmbH
Wittener Straße 45
44789 Bochum
Telefon +49 234 43870-200
info@escrypt.com

www.escrypt.com

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

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

KPMG AG Wirtschaftsprüfungsgesellschaft
THE SQUAIRE
60549 Frankfurt
Telefon +49 69 9587-0

www.kpmg.de
www.kpmg.com/socialmedia

Status: 10/2020