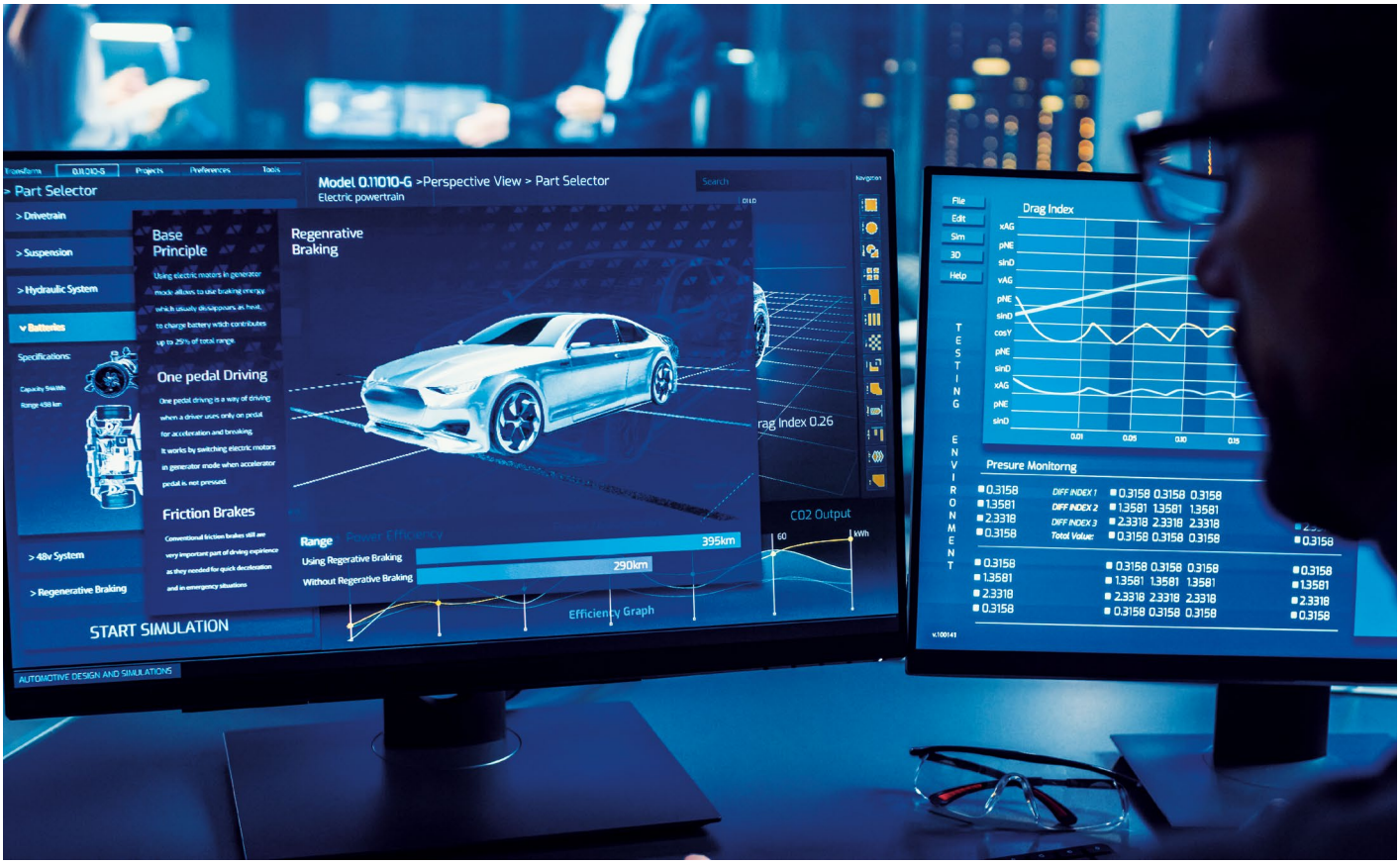
Cyber Security Management – Neue Dimensionen automobiler Sicherheit

UNECE R155/Cyber Security Management System

Vernetzte Fahrzeuge und autonomes Fahren: Für solche automobilen Schlüsselinnovationen gelten seit kurzem neue Regulierungen der UNECE. Zu den wichtigsten Vorgaben gehört die Anforderung, ein normgerecht aufgebautes Cyber Security Management System einzuführen (UNECE R155). Wesentlicher Erfolgsfaktor für die Umsetzung ist ein Umdenken über die Grenzen der Domänenstrukturen hinaus – in Richtung eines ganzheitlichen Ansatzes, der auch die Lieferkette mit einbezieht.

Vernetzte, digitale Funktionen eröffnen Autobauern neue Pfade zu Innovation und Wachstum, die in der aktuellen Umbruchssituation der Branche von existentieller Bedeutung sind. Zugleich schaffen sie aber durch Datenschnittstellen und wachsenden Softwareanteil auch ein neues Einfallstor für Cyber-Bedrohungen, die in einem Fahrzeug durch Ausnutzen von Schwachstellen einen negativen Einfluss auf die physikalische „Safety" mit sich bringen können. Darauf haben die internationalen Regulatoren reagiert und neue Vorschriften verabschiedet, um die Auswirkungen von Cyber-Bedrohungen auf ein gesellschaftlich akzeptierbares Niveau abzusenken. Diese Regulationen werden in absehbarer Zeit verpflichtend für neue Typzulassungen, später für die gesamte Modellpalette. UNECE R155 beinhaltet im Kern die Vorschrift, ein zertifiziertes Cyber Security Management System (CSMS) einzuführen. Hersteller müssen sich dabei darauf einstellen, dass sich mit dem CSMS ihre Verantwortung in neue Dimensionen ausweitet, die bislang noch nicht ausreichend im Blick sind. Denn durch die besondere Natur von Software-basierter Funktionalität ergibt sich eine kontinuierliche Verpflichtung zur Security-Nachbesserung und Gefahren-Abwehr über den ganzen Lebenszyklus des Fahrzeugs: Die Entwicklung endet nicht mit dem „Start of Production" (SOP). Die Fahrzeugflotten im Feld müssen beobachtet und hinsichtlich einer sich ändernden Bedrohungslage durch neu aufkommende Schwachstellen regelmäßig neu bewertet werden. Das CSMS muss auch die Einhaltung von Cyber Security-Anforderungen entlang der kompletten Lieferkette sicherstellen. Keine triviale Anforderung, denn 70 bis 90 Prozent des Software-Bestands eines typischen Fahrzeugs stammen aktuell von Zulieferern. Auch wenn sich dieser Anteil in Zukunft vermutlich zugunsten der OEMs verschieben wird, verdeutlicht der Aspekt, wie komplex und mehrdimensional die Thematik ist. Eine ganzheitliche Sichtweise auf das CSMS ist daher unerlässlich – von der Entwicklung über die Produktion inklusive Lieferkette bis zur Fahrzeugflotte im Feld.



Regulatorischer Anpassungsdruck

Nicht alle OEMs sind auf diese regulatorische Neuerung ausreichend vorbereitet. Zu Beginn der mehrjährigen Zyklen vieler aktueller Entwicklungsprojekte waren die neuen Anforderungen schlicht noch unbekannt. Daher besteht jetzt akuter Handlungsbedarf, um regulatorische Compliance zu gewährleisten. Natürlich haben OEMs darüber hinaus auch ein vitales Eigeninteresse an einem robusten Cyber Security Management System – um Haftungsrisiken zu verringern, Reputationsschäden zu vermeiden und das Ausrollen neuer Daten-getriebener Geschäftsmodelle nicht zu gefährden. Die große Brisanz des Themas ist den Unternehmen spätestens seit dem spektakulären externen Hack eines US-Fahrzeugs über das Infotainment-System mit Zugriff u.a. auf Lenkfunktionen bewusst, der im Jahr 2015 die Branche aufgerüttelt hat. Es handelte sich zwar „nur" um eine Demonstration durch Experten. Unabhängig davon waren die Folgen drastisch: Rückruf von 1,4 Mio. Fahrzeugen, Strafzahlung von 105 Mio. Dollar. Ein weiterer Aspekt erhöht den Handlungsbedarf für OEMs noch zusätzlich: der steigende Wettbewerbsdruck durch neue Marktteilnehmer. Die Architekturen ihrer Fahrzeuge sind oft von vornherein digital konzipiert. Es besteht keine Abhängigkeit von Legacy-Systemen, eine Umsetzung von neuen Cyber-Standards ist für diese OEMs durch fortgeschrittene Software, Update-Fähigkeiten und technologische Agilität wesentlich einfacher. Demgegenüber haben die meisten traditionellen Hersteller Nachholbedarf.

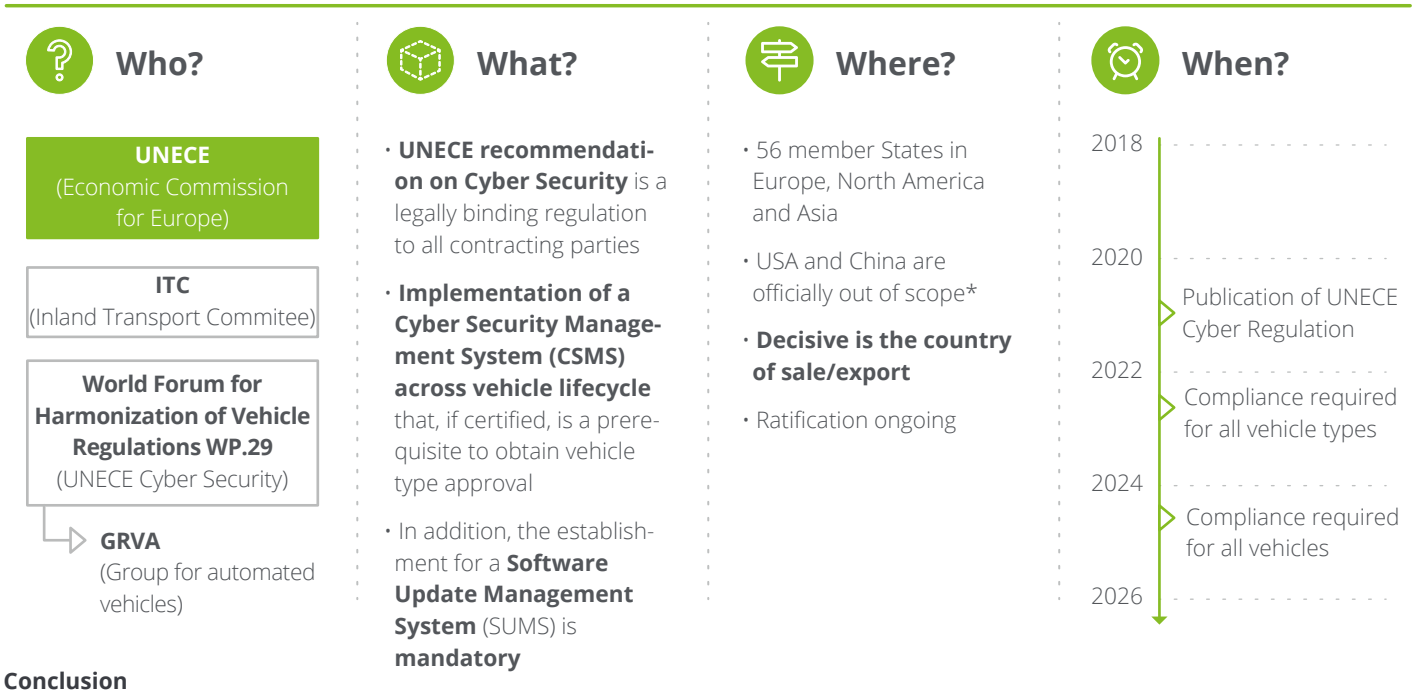
Die neue Regulation ist ein Ergebnis der Arbeit des Weltforums für die Harmonisierung von Fahrzeugvorschriften des Inland Transport Committee (ITC) der Wirtschaftskommission der Vereinten Nationen für Europa (UNECE), bzw. der Untergruppe GVRA für automatisierte Fahrzeuge, kurz der Arbeitsgruppe WP.29. Im Juni 2020 wurde R155 verabschiedet, im Januar 2021 trat sie in Kraft. Ab Juli 2022 sind die Vorgaben verpflichtend für alle neuen Fahrzeugtypen, ab Juli 2024 dann für sämtliche Neufahrzeuge in der EU. Ebenfalls verabschiedet wurde die Regulierung R156, die den Aufbau und Betrieb eines zertifizierten Software Update Management Systems (SUMS) vorschreibt. Weitere Neuregelungen stehen u.a. für das autonome Fahren bevor (Automated Lane Keeping System – ALKS sowie SOTIF-Themenkomplex: „Security of the Intended Function", Sicherheit der Sollfunktion; neues Gesetz zum autonomen Fahren). Diese Aspekte werden in weiteren Ausgaben dieser Point of View-Reihe behandelt, während im Folgenden R155 mit den Vorgaben zum CSMS im Mittelpunkt steht.

> Es besteht akuter Handlungsbedarf, um regulatorische Compliance zu gewährleisten.

Neue Normen mit globaler Relevanz

Auch wenn längst nicht alle Nationen zum UNECE-Geltungsbereich gehören, spricht vieles dafür, dass sich die Regeln zum globalen De-facto-Standard entwickeln werden. Direkt zugehörig sind 56 Mitgliedsstaaten aus aller Welt. Entscheidend ist der Ort des Verkaufs bzw. das Exportziel, so dass auch Fahrzeuge aus Drittländern betroffen sind, sofern sie für einen UNECE-Markt bestimmt sind. Die USA stehen hier zwar als Nicht-Mitglied unmittelbar außen vor. Doch da die für die Zertifizierung des CSMS wichtige Norm ISO/SAE 21434 gemeinsam mit der US-Organisation Society of Automotive Engineers (SAE) entwickelt wurde, sind die Regeln auch für Fahrzeuge für den US-Markt relevant. Auch China gehört nicht zum UNECE-Bereich. Hier müssen sich OEMs dennoch auf vergleichbare Anforderungen einstellen. Es kommen aber zusätzlich noch weitergehende Bestimmungen des China Cyber Security Law dazu, die den Datenschutz, die Informationssicherheit und staatliche Befugnisse betreffen.

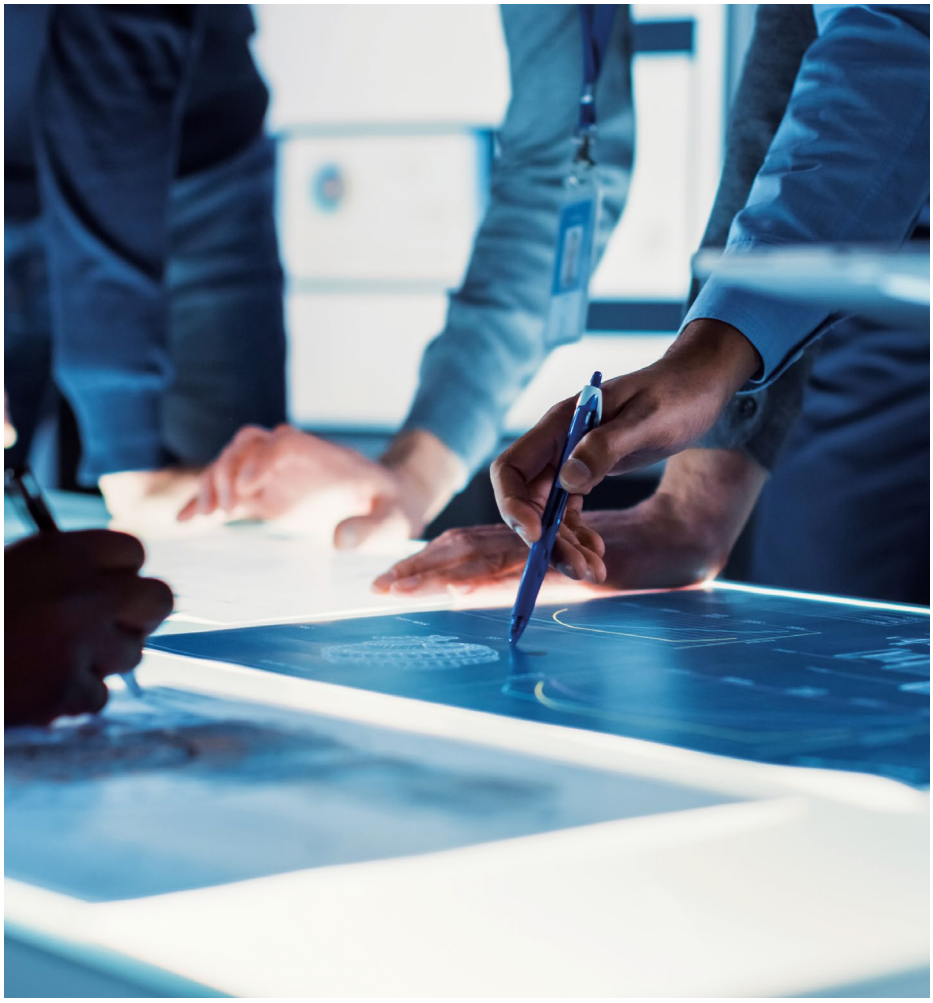
Abb. 1 – UNECE Cyber Regulation in a nutshell



Für die Zertifizierung ist die Einhaltung bestimmter Normen Voraussetzung. Zentrale Bedeutung hat hier die erwähnte Norm ISO/SAE 21434 („Road Vehicles – Cyber Security Engineering"), die u.a. Standards für die Analyse der Bedrohungslage sowie der Risikobewertung setzt und die Entwicklung von Risikomodellen für Onboardsysteme fordert. Schnittstellen und Umfeldsysteme, z.B. in der Cloud, sind Thema u.a. in der ISO 27xxx-Standardreihe. Wichtig sind solche Regeln auch für den Betrieb eines Vehicle Security Operations Center (VSOC) zur Überwachung der Cyber-Lage in der Flotte. Die ISO 31xxx-Reihe bringt weitere Vorgaben zur Risikomodellierung, zur Risikoaggregation und zum Reporting. Zu nennen ist auch der Annex 5 von R155, in dem ausgewählte konkrete Bedrohungen beispielhaft beschrieben sind. Wie ihre Abwehr im Detail technisch zu gestalten ist, wird dabei bewusst offengelassen.

Handlungsfelder für einen ganzheitlichen Ansatz

Cyber Security-Bedrohungen machen nicht an den etablierten Grenzen der verschiedenen Domänen eines OEMs halt. Beim Aufbau eines CSMS kommt es daher wesentlich auf eine kooperative, ganzheitliche Perspektive an, von der Entwicklung eines Fahrzeugs bis zum Monitoring der Flotte. Die Umsetzung erfordert Maßnahmen auf mehreren organisatorischen Ebenen: Governance, Zusammenarbeit, Fahrzeugprojekte. Für eine adäquate Governance ist es notwendig, geeignete Prozesse zur Identifizierung von Risiken in Onboard- und Offboardsystemen zu entwickeln und den Zugriffsbereich des CSMS im Unternehmen abzustecken. Das Programm sollte dann zweitens in einer Zusammenarbeit der einzelnen Domänen umgesetzt und dafür zunächst in diese hineingetragen werden: Entwicklung, Qualitätsmanagement, Lieferantenmanagement, Homologation, IT sowie Kundenanlaufstellen wie Sales, Aftersales und Werkstätten. Diese verschiedenen Bereiche der Wertschöpfung zusammenzuführen ist eine große Herausforderung, da sie bislang eher autark arbeiten. Doch für die Erkennung, Lösung und Verhinderung von Cyber-Vorkommnissen ist Kooperation unerlässlich. Im Blickwinkel des Enterprise Risk Management besteht durch R155 darüber hinaus auch explizit eine Verantwortung des Vorstands, der an dem CSMS-Programm beteiligt werden muss. Damit stellt sich die weitere Herausforderung, aus den genannten operativen Prozess- und Produktrisiken eine Risikoaggregation und -bewertung für den Vorstand abzuleiten. Als organisatorische Maßnahme verleihen viele Unternehmen dem CISO Zuständigkeit für dieses Thema, andere schaffen neue Rollen wie den Chief Product Security Officer (CPSO). In diesem Zusammenhang sind auch die Themen Software-Fähigkeiten und Talent-Management zu beachten. Denn die entsprechenden digitalen Skills liegen oft noch nicht ausreichend im Unternehmen vor, und eine entsprechende Rekrutierung gestaltet sich auf dem derzeitigen Arbeitsmarkt nicht einfach.



Auf der dritten Ebene müssen die neuen Prozesse und Kontrollen schließlich auch konkret in die Fahrzeugprojekte einfließen. Wie das in der Entwicklung geschehen soll, ist durch klare Strukturen zu regeln. Bei Neuentwicklungen, die derzeit in den Markt gebracht werden, ergeben sich akute Herausforderungen durch den langen Zeitvorlauf. Die Fahrzeuge befanden sich schon lange in Entwicklung, als sich die Regeln zum CSMS in den letzten 1-2 Jahren herauskristallisierten. Das führt zwangsläufig zu Lücken, die nun umgehend gefüllt werden müssen. Wichtig ist grundsätzlich, einerseits ein zertifiziertes CSMS aufzubauen und einzusetzen, andererseits aber auch den Nachweis zu erbringen, dass die Kontrollsysteme in den einzelnen Fahrzeugprojekten tatsächlich angewendet werden. Eine revisionssichere Dokumentation ist daher wesentlich. Deloitte hat in diesem Zusammenhang gute Erfahrungen mit selbst entwickelten Dienstleistungen gemacht, mit denen die Effektivität von Maßnahmen in den Projekten nachgewiesen werden kann. Das CSMS hat zudem Implikationen für die Fahrzeugarchitektur, bis hin zu Steuergerätearchitekturen und Funktionsdesign. Die Entwicklung sollte immer dem „Security by design"-Prinzip folgen, das Security-Pflichtenheft ist frühzeitig gegen das Safety-Pflichtenheft abzugleichen. Weitere Herausforderungen resultieren aus dem großen Anteil von Software und den komplexeren Supply Chains: Lieferanten haben die neuen Vorgaben ebenfalls zu erfüllen. Bei neuen und schon laufenden Projekten müssen die Software-Qualität stringent kontrolliert und CSMS-Vorgaben bis zur Code-Ebene hinab umgesetzt werden – ein Bereich, in dem das schon erwähnte SUMS relevant wird, denn auch beim Implementieren von Updates und Bugfixes sind Cyber-Regeln zu beachten. Im Bereich der Typzulassungen wird in diesem Zusammenhang ebenfalls Neuland betreten: „Delta-Zulassungen" aufbauend auf früheren Typen sind angesichts der fundamentalen Neuerungen nicht möglich.

Ausblick: Der regulatorische Diskurs

Die neuen CSMS-Vorgaben von R155 und den anderen relevanten Regulationen sind zwar schon erlassen. Doch bei weitem nicht alle zukünftig relevanten Aspekte sind schon geklärt. In vielen Bereichen befindet sich die nationale Anwendung der UNECE-Regulationen noch im Fluss. Nicht nur für OEMs, sondern auch für nationale Regulatoren und Kontrolleure bringen die Vorgaben Herausforderungen mit sich, denn ihre konkrete Ausgestaltung der Vorgaben muss für OEMs verständlich und praktisch umsetzbar sein. Deshalb laufen schon seit einiger Zeit Probe-Assessments durch Prüfungsorganisationen/technische Dienste bei den Herstellern. Aus solchen Probeläufen gewonnene Erkenntnisse fließen in Form von Anpassungen wieder in die Regulationstexte ein. Auch bezüglich der Hauptuntersuchung besteht noch Klärungsbedarf – etwa hinsichtlich der Frage, bis zu welchem Grad sie in Zukunft digitalisiert ablaufen wird und ob die Anforderungen aus R155 und R156 in die Untersuchungen (z.B. aktuelle Software-Versionen und Bugfixes eingespielt?) einfließen sollten. Im Raum steht außerdem die Option kontinuierlicher Erhebung von Prüfdaten, z.B. von Sensoren zur Messeung deren Qualität bzw. Degradation. Der Zugriff auf Datenpunkte könnte in bestimmten zeitlichen Rhythmen geschehen, oder Event-getrieben auf der Basis bestimmter Schwellenwerte. Durch solche Ansätze kann eine Leistungsverschlechterung von Sensoren durch Abnutzung oder Verschmutzung im Betrieb überwacht werden. Hier wird in naher Zukunft erneut die SOTIF-Thematik relevant, im Moment ist die rechtliche Lage noch nicht klar. Deloitte verfolgt diese Entwicklungen intensiv, z.B. durch Beteiligung an internationalen regulatorischen Gremien und durch einen Austausch mit relevanten deutschen Institutionen wie dem Kraftfahrt-Bundesamt (KBA), den TÜV-Organisationen samt nachgelagerter Instanzen und dem Bundesamt für Sicherheit in der Informationstechnik (BSI). Einschlägig sind hier auch die Erfahrungen der Deloitte Certification Services GmbH mit ihrem breiten technischen Prüfwissen.

Die regulatorischen Entwicklungen rund um das CSMS, ihre operativen Auswirkungen und strategischen Implikationen – ein unübersichtliches Feld, das in Bewegung ist und bleibt. Aber auch wenn noch nicht sämtliche regulatorischen Details abschließend festgezurrt sind: Für Hersteller ist es nun höchste Zeit zu handeln. Sie müssen im Lauf des Jahres 2021 ihr CSMS zertifizieren lassen, sonst sind gemäß R155 die Typzulassungen gefährdet. Ebenso ist laut R156 die Einführung eines Software Update Management Systems (SUMS) Pflicht. Diesem nicht weniger dringenden Thema widmet sich der zweite Point of View dieser Reihe.

Der erste Schritt: Deloitte Vehicle Cyber Security Readiness Assessment

Zur Vorbereitung auf die neue regulatorische Wirklichkeit ist zunächst eine umfassende Bestandsaufnahme geboten. Hierbei bietet sich Unterstützung durch unabhängige Dritte an, die einen neutralen, kritischen Blick mitbringen. Die Experten von Deloitte haben dafür ein Readiness Assessment im Rahmen des Deloitte Automotive Cyber Security Frameworks entwickelt, mit dem ein einheitlicher Stand im Unternehmen hergestellt werden kann. Dieser Ansatz basiert auf den Erfahrungen aus Projekten mit einer Vielzahl von OEMs, aus denen u.a. ein umfangreicher CSMS-Fragenkatalog erstellt wurde. Organisationen haben in dieser Lage typische Schwierigkeiten: Fehlendes Compliance-Monitoring, mangelnde Transparenz, Verzögerungen bei der Umsetzung und fehlende Risiko-Identifikationsprozesse führen zu Problemen, die eine Zertifizierung des CSMS und damit die Zulassung gefährden können. Deshalb ist es nötig zu klären, wie das eigene Unternehmen im Hinblick auf die Regulationen aufgestellt ist, welche Konsequenzen eine fehlende Compliance haben könnte und welche Lücken zu schließen sind. Wie kann Cyber Security Readiness weltweit erreicht werden, und wie steht der Hersteller im Vergleich zu Wettbewerbern da?

Das Cyber Security Readiness Assessment erfasst im ersten Schritt den Ist-Zustand mit Dokumentenreviews, aus denen sich Diskussionspunkte für anschließende Interviews und Workshops ergeben. Durch Deep Dives wird die Analyse detailliert, bestehende Lücken im Unternehmen können identifiziert werden. Ein Abgleich mit Deloittes Reifegrad-Modell bietet einen objektiven Maßstab für die Beurteilung. Eine Roadmap und Handlungsempfehlungen füllen die Gap-Analyse mit umsetzbaren Lösungen. Nach einer Zwischenvalidierung der Ergebnisse wird abschließend ein umfangreicher Assessment Report mit Management Summary und Maßnahmenlisten erstellt. Das gesamte Vorgehen wird dabei Audit-konform dokumentiert. Ein „Friendly Audit" durch Deloitte ist eine zusätzliche Option.

Kontakte

Ingo Dassow
Director | Risk Advisory
Automotive Cybersecurity
Tel: +49 (0)151 58801451
idassow@deloitte.de

Andreas Herzig
Partner
Automotive Lead Risk Advisory
Tel: +49 (0)711 16554 7160
aherzig@deloitte.de

Anke Guderian
Director | Risk Advisory
Automotive Software Governance
Tel: +49 (0)89 29036 6212
aguderian@deloitte.de

Deloitte.

Stand 03/2021