Presseinformation

FEV stellt holistischen Ansatz gegen Cyberattacken auf Fahrzeuge vor

Medienkontakt
Ulrich Andree
T +49 241 5689-8880
andree@fev.com

www.fev.com

Aachen / Auburn Hills (Michigan, USA), Februar 2021 – FEV, ein weltweit führender Dienstleister in der Fahrzeug- und Antriebsstrangentwicklung für Hard- und Software, hat den zunehmenden Einsatz von Software in Fahrzeugen als ein erhebliches Cybersecurity-Risiko identifiziert. Das Unternehmen hat aus diesem Grund eine neues, sogenanntes „SPORT-Framework" entwickelt („SPORT" steht für Strategie, Prozess, Organisation, Ressourcen und Technologie), das es OEMs und Zulieferern ermöglicht, Hackern einen Schritt voraus zu sein.

Das FEV SPORT-Framework wurde entwickelt, um das Thema Cybersecurity holistisch zu adressieren. **Strategie** berücksichtigt die Unternehmensvision, -mission und -kultur des OEMs oder Zulieferers. Dieser Schritt gleicht die Cybersecurity-Strategie mit der Unternehmensstrategie ab und beschreibt deren Auswirkungen auf das aktuelle und zukünftige Produktportfolio sowie auf die Kundenbasis.

Prozess umfasst Entwicklungsprozesse, beispielsweise den sogenannten „Security Development Life Cycle" und das Wissensmanagement, sowie Audit- und Trainingsprozesse, unterstützt durch einen dedizierten Change-Management-Workstream.

Organisation befasst sich mit der Struktur der Cybersecurity-Teams und entwickelt eine Berichtsstruktur mit klaren Rollen und Verantwortlichkeiten, während **Ressourcen** die notwendige

Teamgröße definiert und sich um die Personalrekrutierung und Outsourcing-Strategien kümmert.

Technologie umfasst

- Eine hochsichere Hard- und Softwarestrategie
- Technische Maßnahmen (konstruktiv und analytisch)
- Verfügbare Tools und Infrastruktur

Die Entwicklung der Automobilindustrie und die zunehmende Implementierung von Informationstechnologie in die Fahrzeuge haben das SPORT-Framework von FEV zu einem wertvollen Service für die Automobilhersteller gemacht. Denn im Jahr 2010 verfügte ein Premium-Fahrzeug noch über bis zu 100 Millionen Zeilen Software-Code, heute sind es bereits fast 150 Millionen Zeilen. Bis 2030 wird erwartet, dass dieser Wert auf über 300 Millionen steigen wird. Der Anstieg an Software-Inhalten bedeutet gleichzeitig eine Zunahme potenzieller Angriffspunkte für Cyberattacken.

In den letzten Jahren hat die Bedeutung von Cybersecurity bereits ihren Weg in die Jahresabschlüsse großer Unternehmen der Automobil- und Technologiebranche gefunden. Eine Handvoll öffentlichkeitswirksamer Angriffe hat unmittelbar zu einem Rückgang der Aktienkurse geführt und eine Beeinträchtigung der Geschäftsentwicklung sowie der Unternehmensreputation nach sich gezogen. So führte eine Cyberattacke im Jahr 2015 zu einem Rückruf von fast 1,5 Millionen Fahrzeugen. In Folge entstanden geschätzte Kosten von etwa 600 Millionen US-Dollar und dem betroffenen OEM ein geschätzter Verlust seines Börsenwertes von 4 Milliarden US-Dollar.

Mit zunehmender Komplexität der Fahrzeuge steigt künftig die Gefahr solcher Ereignisse sogar noch. Zudem triggern die im Fahrzeug zunehmend gespeicherten und abrufbaren Verbraucherinformationen Cyberattacken.

“Cybersecurity wird in den kommenden Jahren eine immer wichtigere Rolle für globale Automobilhersteller spielen – gerade vor dem Hintergrund zunehmend vernetzter und automatisierter Fahrzeuge“, sagt Mayank Agochiya, Geschäftsführer von FEV Consulting, Inc.

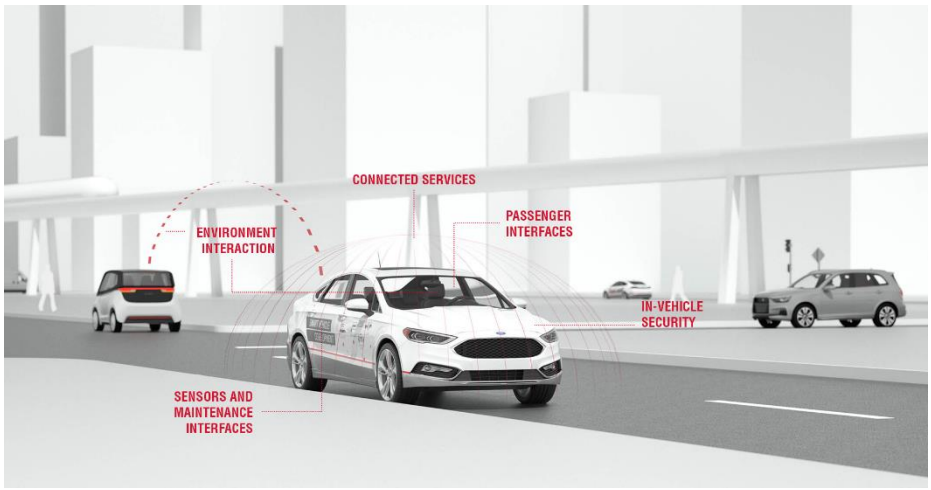
Weiterhin stellen Cybersecurity-Maßnahmen aber auch eine Chance zur Differenzierung dar. Da Fahrzeugbesitzern und -nutzern hochintegrierte Konnektivitätsfunktionen angeboten werden, wird Vertrauen in diesem Zusammenhang eine wichtige Rolle bei der Akzeptanz spielen.

Die Mobilitätsbranche wird daher ihr Augenmerk verstärkt auf Cybersecurity richten. So wird erwartet, dass die Einhaltung der meisten Cybersicherheitsvorschriften und -standards (einschließlich ISO 21434) für all Fahrzeuge mit Markteinführung im Jahre 2025 angestrebt wird. Mit dem Inkrafttreten von UNECE WP.29 wird die Cybersicherheit in 54 Ländern sogar bereits vor 2025 ein obligatorischer Aspekt der Typgenehmigung werden.

„Um diese Anforderungen zu erfüllen, müssen OEMs und Zulieferer frühzeitig handeln, um bis spätestens 2025 handlungsfähig zu sein“, sagt Agochiya. „Hierfür gilt es, komplexe Cybersecurity-Organisationen, -Ressourcen und -Prozesse bis Ende 2022 aufzubauen. Mit unserem SPORT-Framework setzen wir genau an dieser Stelle an und unterstützen unsere Kunden darin, sichere Fahrzeuge zu entwickeln.“

Der Ansatz von FEV hat sich bereits bei der Identifizierung und Entschärfung von Risiken bewährt. Das holistische SPORT-Framework ermöglicht es OEMs und Zulieferern, dank vorausschauender und zielgerichteter Maßnahmen sowohl ihr Geschäft vor Cyberangriffen zu schützen als auch die Sicherheit der Fahrzeugnutzer zu erhöhen.

https://www.fev-consulting.com/de.html



Dank vorausschauender und zielgerichteter Maßnahmen ermöglicht es das FEV eigene, ganzheitliche SPORT-Framework OEMs und Zulieferern, sowohl ihr Geschäft vor Cyberangriffen zu schützen als auch die Sicherheit der Fahrzeugnutzer zu erhöhen.
Quelle: FEV Group

Über FEV
FEV ist ein international führender, unabhängiger Dienstleister in der Fahrzeug- und Antriebsentwicklung für Hardware und Software. Das Kompetenzspektrum umfasst die Entwicklung und Erprobung innovativer Lösungen bis hin zur Serienreife sowie angrenzenden Beratungsleistungen. Zum Leistungsumfang auf der Fahrzeugseite gehören die Auslegung von Karosserie und Fahrwerk, inklusive der Feinabstimmung der Gesamtfahrzeugattribute wie Fahrverhalten und NVH. Zudem werden bei FEV innovative Lichtsysteme und Lösungen zum autonomen Fahren sowie Connectivity entwickelt. Bei der Elektrifizierung von Antrieben entstehen leistungsfähige Batteriesysteme, e-Maschinen und Inverter. Darüber hinaus werden hocheffiziente Otto- und Dieselmotoren, Getriebe, EDUs sowie Brennstoffzellensysteme entwickelt und unter Berücksichtigung der Homologation ins Fahrzeug integriert. Ein weiterer Schwerpunkt sind alternative Kraftstoffe.

Das Leistungsangebot wird abgerundet durch maßgeschneiderte Prüfstände und Messtechnik sowie Softwarelösungen, durch die wesentliche Arbeitsschritte der oben genannten Entwicklungen effizient von der Straße in den Prüfstand oder in die Simulation verlegt werden können.

Die FEV Gruppe wächst kontinuierlich und beschäftigt aktuell 6.700 hochqualifizierte Spezialisten in kundennahen Entwicklungszentren an mehr als 40 Standorten auf fünf Kontinenten.

Über FEV Consulting

FEV Consulting, mit Hauptsitz in Aachen und weiteren Büros in München, Köln, Bilbao, Peking, Dubai und Auburn Hills, kombiniert die Kompetenz der Top-Management-Beratung mit den technischen Fähigkeiten und dem Know-how der FEV Group. Durch tiefe Branchenkenntnis entwickelt FEV Consulting pragmatische Lösungen für einige der drängendsten und komplexesten Probleme, denen Unternehmen heute weltweit gegenüberstehen.

FEV Consulting bietet einzigartige, kundenorientierte Beratungsleistungen durch jahrelange Erfahrung in der Unternehmensberatung. Das Unternehmen adressiert die Herausforderungen seiner Kunden mit seinem analytischen Ansatz, bewährten Fähigkeiten sowie umfassenden Branchenkenntnissen, und erarbeitet kundenspezifische Lösungen.