Automotive Cyber Security Management System

Autoren:

Dr. Michael W. Müller
Dino Munk
Magility Cyber Security GmbH, Wendlingen am Neckar, Deutschland

Zusammenfassung

Die Cyberkriminalität betrifft nicht nur Großunternehmen, sondern auch die Zivilgesellschaft, kleine und mittelständische Unternehmen und die öffentliche Verwaltung. Die deutsche Polizei erfasste im Jahr 2022 mehr als 100.000 Fälle von Cyberkriminalität in Deutschland. Die Automobilindustrie erlebt aktuell einen massiven digitalen Wandel, der durch die Verbreitung von "Software defined vehicles" und die Entwicklung neuer digitaler Mobilitätskonzepte vorangetrieben wird. Cyber-Security ist zu einem kritischen Teil der Hard- und Software Wertschöpfungskette geworden und wird heute ernster denn je wahrgenommen. Mit zunehmender Anzahl vernetzter Fahrzeuge steigen auch die Risiken für die OEM. Automotive Cyber-Angriffe haben Auswirkungen in unterschiedlichen Gefährdungsstufen, bedrohen im schlimmsten Fall Menschenleben und gefährden die öffentliche Sicherheit. Ein umfassender Cyber Security Schutz über den gesamten Lebenszyklus der Fahrzeuge wurde unerlässlich. Die Regulierung Nr. 155 der UNECE (UNECE R-155) definiert die Anforderungen an das Cyber Security Management System (CSMS) der OEMs und schreibt vor, dass Automobilhersteller für die Fahrzeug Typzulassung nachweisen müssen, dass sie ihre Fahrzeuge und Flotten vor Cyberangriffen schützen können.