VICCON

CONSULTING

Automotive Security Management

Ein innovativer Ansatz für die Weiterentwicklung des Sicherheitsmanagements in der Automobilbranche

IMPRINT

Broschüre Automotive Security Management - Ein innovativer Ansatz für die Weiterentwicklung des Sicherheitsmanagements in der Automobilbranche

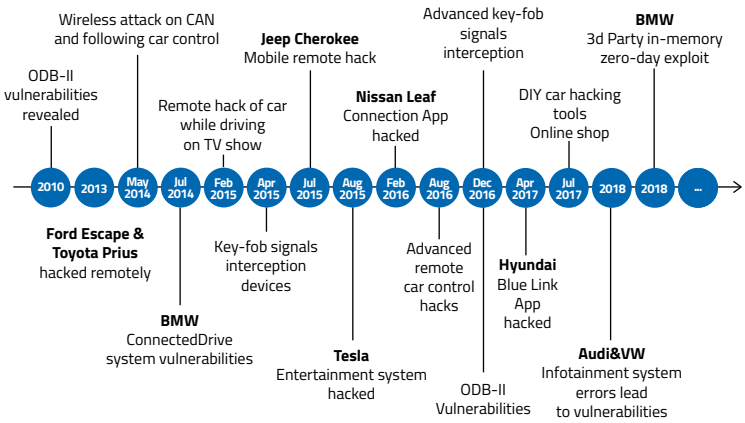
© 2019 VICCON GmbH

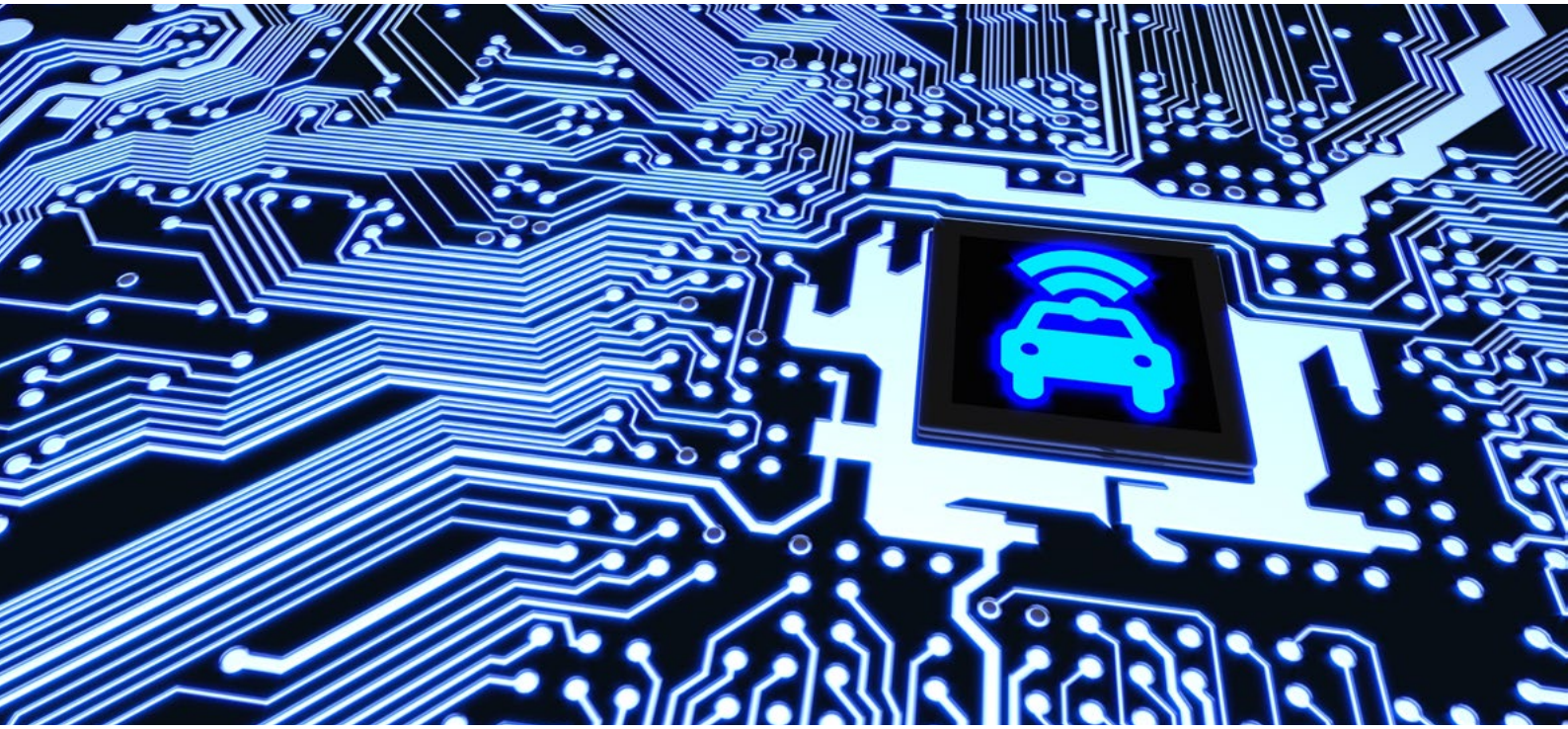
Die verschiedenen Vorfälle der Hacking Timeline zeigen, dass es ein Bedrohungspotential für Automotive im Cyberraum gibt

Die Transformation der Automobilbranche schreitet zügig voran. Die wesentlichen vier Trends in Mobility sind: Electrified, Connected, Automated, Shared. Auf diese Herausforderungen muss die Branche Antworten finden. Dies ist nur möglich mit digitalisierten und kommunizierenden Automobilen, den sogenannten Connected Cars. Connected Cars bedeutet auch die Verbindung zwischen Systemen, die sich nicht vertrauen. Dies setzt ein ausreichendes Maß an Cyber Security voraus, denn durch stärkere Vernetzung, zusätzliche Schnittstellen und Funktionalitäten wird die Attraktivität eines Angriffes auf Fahrzeuge und die angebundene Infrastruktur durch Hacker drastisch erhöht.

Die verschiedenen Vorfälle der Hacking Timeline zeigen, dass es ein Bedrohungspotential für Automotive im Cyber-Raum gibt. Dieses Bedrohungspotential ist heute möglicherweise nur durch einzelne Komponenten gegeben, aber wird durch die Digitalisierung und Vernetzung rasant wachsen. Hackergruppen wie Group123, Dark Hotel oder Mofang sind nach Expertenmeinung im Automobilsektor aktiv. Sehr weit entwickelten Hackergruppen steht eine Branche entgegen, die Digitalisierung, Kommunikation und Vernetzung nun erst in voller Breite und Tiefe nutzen wird.

Und Konnektivität bedeutet nicht nur die Verbindung von Fahrzeugen mit dem Internet oder mit anderen Fahrzeugen, sondern unter Umständen auch mit dem Elektrizitätsnetz. Elektrische Fahrzeuge könnten zukünftig auch Teil des Stromnetzes werden und kommunizieren dann auch mit dieser Technologie. Sie könnten, von Hackern gesteuert, somit selbst zum Angriffsvektor auf die Stromversorgung werden. Entsprechende Betrachtungen existieren.





Connected Cars wird solchen Bedrohungssituationen somit ein rasantes Wachstum bescheren. Dabei können die Angriffsvektoren hinsichtlich der Auswirkungen bei der Fahrzeug- oder Komponentenproduktion nicht mehr nur einer Unternehmens- oder IT-Domäne zugeordnet werden. Schaut man auf den Entwicklungsprozess im Unternehmen, so kann ein Angriff auf die Software-Entwicklungsumgebung für Fahrzeugkomponenten, die in der Bürokommunikationsumgebung betrieben wird, später zu Fehlfunktionen einer Komponente im Fahrzeug führen. Schutzanforderungen, die nur in einer Abteilung, einer Domäne oder einer Produktionseinheit definiert sind und nicht einer ganzheitlichen Betrachtung und Steuerung unterworfen sind, werden langfristig nicht wirksam sein und scheitern.

Dies sieht auf Ebene eines Fahrzeugs nicht anders aus. Ein Fahrzeug besteht aus verschiedenen digitalen Domänen wie zum Beispiel Chassis Control, Body Control, Assistenzsysteme oder Infotainment, von denen einige sicherheitsrelevant sind, andere nicht. Alle Systeme konsumieren oder erzeugen Daten. Um diese digitalen Funktionen zu kontrollieren und zu steuern, haben die typischen Automobile der aktuellen Dekade über 100 Mikroprozessoren, mehrere Dutzend elektronische Kontrolleinheiten, mehrere Kilometer Kabel und an die 100 Millionen Zeilen Softwarecode. Unerkannte Schwachstellen sind somit unvermeidlich. Ein übergreifendes Bedrohungs- und Schwachstellenmanagement muss ebenso existieren wie ein Vorfallbehandlungsprozess.

Darüber hinaus werden sicherheitsrelevante Systementwicklungen immer komplexer, was zu immer größeren Anforderungen an die Hersteller und ihrer Lieferanten führt. Zur Erlangung der notwendigen Produktsicherheit ist gemäß dem Stand der Technik zu entwickeln, um etwaigen Produkthaftungsansprüchen vorbeugen zu können. Es gilt, die Funktionale Sicherheit der entsprechenden Produkte, Systeme und Prozesse sicherzustellen. Sicherung leistet einen Beitrag dazu.

Sicherheits-relevante System-entwicklungen werden immer komplexer

VEHICLE SECURITY

Vehicle Security umfasst die Elemente, die zum sicheren Betrieb eines Fahrzeugs notwendig sind

Sicherheit bzw. Safety bedeutet der Schutz von Mensch und Umwelt. Sicherung bzw. Security bedeutet der Schutz vor schädigenden Handlungen. Datenschutz bzw. User Data Privacy schützt personenbezogene Daten vor Missbrauch. Betrachtet man die Funktionsweise von Fahrzeugen, so ist auch unter Verwendung digitaler Komponenten die Funktionale Sicherheit (Functional Safety) von Fahrzeugen, Fahrzeugteilen, Produkten und Services sicherzustellen. Die Sicherung (Security) schützt dabei die betrieblichen und sicherheitstechnischen Funktionen eines Fahrzeugs sowie die Privatsphäre der Nutzer des Fahrzeugs.

Vehicle Security umfasst die Elemente, die zum sicheren Betrieb eines Fahrzeugs notwendig sind, insbesondere bei automated bzw. autonomous vehicles. Hinzu kommen eingekaufte Komponenten oder Services eines Zulieferers und Teile der Lieferkette, die sich auf digitale Elemente beziehen. Diese Komponenten, Services oder Teile unterliegen ebenso zahlreichen Cyber-Risiken, die in einem Hersteller oder Integrator nicht bekannt sind und durch ein Sicherheitsmanagement gesteuert werden müssen. Hinzu kommen Wartung und Betrieb von Komponenten, Services oder Fahrzeugen, die gegebenenfalls personenbezogene Daten produzieren, die dann speziell zu schützen sind. Internetbezogene Geräte und Apps (IoT Devices), die mit Fahrzeugen oder Produkten kommunizieren oder interagieren sind Beispiele dafür.

AUTOMOTIVE SECURITY MANAGEMENT

ASMS

ist ein umfassender und erfolgversprechender Ansatz

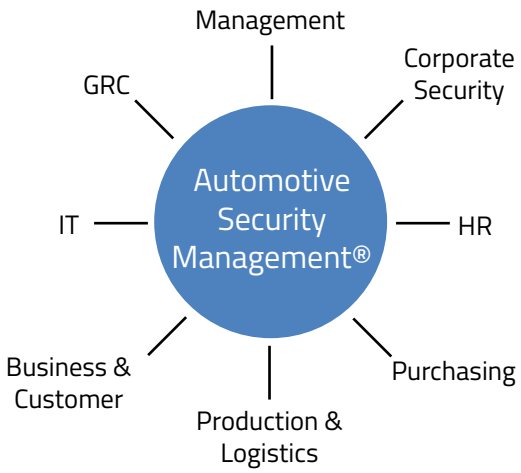
Im Automobilsektor werden aktuell neue Ansätze und Ideen diskutiert, wie ein unternehmensübergreifendes Sicherheitsmanagement erreicht werden kann. Der Bedarf ergibt sich aus dem notwendigen Zusammenwirken von unterschiedlichen Unternehmenseinheiten, der gemeinsamen Zielsetzung nach dem Schutz Funktioneller Sicherheit sowie der Konnektivität und Verschmelzung der digitalen Systeme mit der Business-IT. Somit wird ein Sicherheitsmanagementansatz gesucht, der die Bereiche Business, Produktion und Produkt miteinander verbindet. Gleichzeitig existieren zahlreiche Anforderungen an Hersteller und Zulieferer, die sich zum Beispiel aus Datenschutz, Zertifizierungen oder Compliance-Audits ergeben können wie zum Beispiel bei ISO 27001 oder TISAX, für die VICCON eine Risikoanalysemethode entwickelt hat. Hinzu kommen internationale Rahmenwerke wie das der UN ECE, das Vehicle Security und Produkthaftung beeinflusst.

VICCON verfolgt einen übergreifenden Ansatz in Form eines Automotive Security Management System® (ASMS) für Automobilhersteller und Automobilzulieferer, das die Lieferkette berücksichtigt. Die Produktion eines Fahrzeugs oder einer Fahrzeugkomponente kann in verschiedene Phasen unterteilt werden, die eng mit Geschäftsprozessen interagieren. Ein gemeinsamer und effizienter Schutz über alle Geschäftseinheiten und Produktionsstandorte sollte gegeben sein, um das übergreifende Ziel eines sicheren digitalisierten Produkts zu erreichen. Dazu werden existierende und kommende Standards für Cyber Security und Informationssicherheit verbunden und angewendet.

Automotive Security Management System®			
Business Process Information Security Knowledge Protection / Information Security / Data Protection			
Concept	Product Development	Production	Operation, Maintenance
Protection of Prototypes	Protection of Engineering Systems	Protection of Production Systems/Machines	Protection of Operational Systems / Maintainance Data

DIGITALES VERTRAUEN UND SICHERHEITSSTRATEGIE

Die Herstellung von Fahrzeugen oder Fahrzeugkomponenten beschränkt sich natürlich nicht auf die rein digitalen Aspekte. Die Steuerung weltweit verteilter Geschäftsprozesse an verschiedenen Standorten, einer weltweiten Logistik und der Umgang mit verschiedenen Kulturen und reisenden Mitarbeitern erfordert ein umfassendes Sicherheitsmanagement auf Unternehmensebene, verbunden mit den Funktionen Governance, Risk, Compliance (GRC). Das Management und die fachlichen Unternehmensschnittstellen müssen bedient werden und entsprechende Prozesse und Instrumente weiterentwickelt und zueinander angepasst werden. Darüber hinaus stellt sich die Frage, wie Bewusstseinsbildung, Wissenstransfer, agiles Arbeiten und Kollaboration bei der Schnelllebigkeit von Trends, Produkten und Arbeitsverhältnissen sinnvoll organisiert werden können.



Der vom Kunden wahrgenommene Wert von materiellen Gütern verschiebt sich zu Gunsten von immateriellen Gütern und Services. Fahrzeugbezogene Services müssen regional und international verfügbar sein, sicher funktionieren und verlässig bereitstehen. Dies erfordert die Zusammenarbeit vieler Bereiche. Neue Fähigkeiten müssen in bestehende Strukturen integriert werden. Eine höhere Komplexität, echtzeitfähige Reaktionen und vielfältige Wünsche sind der Preis der modernen, digitalen Welt.

Trends und Themen wie Industrie 4.0, Digitales Vertrauen, Resilienz, Vernetzte Gesellschaft und New Work müssen in zukünftige Überlegungen einfließen. VICCON verarbeitet solche Anforderungen in einer Sicherheitsstrategie, in der mit einem methodischen Ansatz konkrete Maßnahmen für die zukünftige Arbeit der Sicherheitsabteilungen und des gesamten Unternehmens abgeleitet werden.

Strategisches Vorgehen

berücksichtigt relevante Anforderungen, Trends und Entwicklungen und ermöglicht einen zukünftigen Blick auf Sicherheit

ADVICE - DIALOG - KNOWLEDGE TRANSFER - IMPLEMENT - EDUCATE

VICCON unterstützt seit rund 20 Jahren Organisationen darin, sicherheitsrelevante Entwicklungen zu verstehen, die notwendigen Kompetenzen und Prozesse dafür aufzubauen und sie so sicher zu beherrschen.

VICCON entwickelt mit Ihnen gemeinsam Ideen und sucht im Dialog mit allen Unternehmensebenen eine passende Orientierung zur Sicherheitspolitik im Lichte der unterschiedlichen Anforderungen.

VICCON entwickelt Strategien für sichere und resiliente Organisationen, begleitet die digitale Transformation und berät bei der Implementierung dieser Strategien in Form eines Next Generation Security Managements.

VICCON verfolgt das Ziel, Security im Sinne des Managements und Business im Unternehmen strategisch zu verankern. Besondere Schwerpunkte liegen im Informationssicherheitsmangement sowie im Management von Cyber-Risiken und im Prototypen- und Know-how-Schutz.

KONTAKT

Für weitere Informationen kontaktieren Sie:

VICCON GmbH

Ottostraße 1
76275 Ettlingen
Deutschland

Tel.: +49 7243 719734
Fax: +49 7243 719704

E-Mail: info@viccon.de
www.viccon.de

VICCON

CONSULTING