NEWS RELEASE

Pressemeldung (Sperrfrist, 27.2.2024, 9:30)

Cybersicherheit: Immer mehr Angriffe auf Automobilbranche

Studie zu Automotive Cyber Security

Prof. Dr. Stefan Bratzel

Center of Automotive Management (CAM)

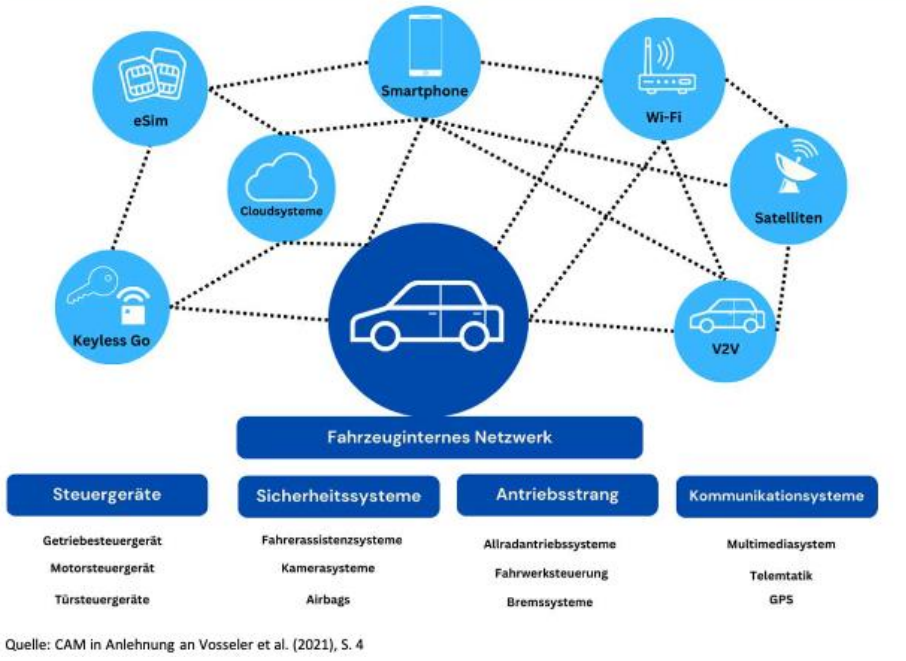
Bergisch Gladbach, den 31.01.2024

- Die Bedeutung von Cyber Security steigt mit Digitalisierung und Vernetzung der Fahrzeuge, Elektromobilität und autonomem Fahren
- Immer mehr Cyber-Angriffe auf Fahrzeuge und Unternehmen erhöhen permanent die Gefahrenlage
- Umfassende Cybersicherheitsstrategien sind heute nötig, werden aber nicht überall umgesetzt

Cyber Security zählt zu den größten Herausforderungen und Erfolgsfaktoren der Automobilbranche in den nächsten Jahren. Mit zunehmender Digitalisierung und Vernetzung der Fahrzeuge sowie den Trends Elektromobilität und autonomes Fahren wächst der Bedarf für eine effektive Cybersicherheitsstrategie. Fahrzeuge und Unternehmen der Automobilwirtschaft sind verstärkt Ziele von Cyber-Angriffen. Die stark zunehmenden Risiken zeigen die Dringlichkeit für umfassende Cyber-Security-Programme. Doch die Qualität ihrer Konzeption und Umsetzung ist in den verschiedenen Wertschöpfungsebenen und -stufen der Branche sehr unterschiedlich. Das zeigt die Studie „Automotive Cyber Security“, die vom Center of Automotive Management (CAM) in Kooperation mit Cisco Systems verfasst wurde.

Mit der zunehmenden Vernetzung und Digitalisierung von Autos, Produktion und Logistik, steigt das Risiko für Cyberangriffe auf die Automobilindustrie. In einer umfassenden Analyse wurden die verschiedenen Angriffsvektoren systematisch analysiert. Allein beim vernetzten Fahrzeug gibt es 12 verschiedene Angriffsbereiche, in denen wiederum potenziell mehrere Eintrittsmöglichkeiten bestehen.

Abb. 1: Angriffspunkte des vernetzten Fahrzeugs



Quelle: CAM in Anlehnung an Vosseler et al. (2021), S. 4

Die Aufstellung zeigt weiterhin: Cyberangriffe beschränken sich in der Automobilindustrie nicht auf große, etablierte Hersteller, sondern treffen verstärkt Zuliefererunternehmen, Automobilhändler und weitere Player entlang der Wertschöpfungskette. Eine Analyse von 52 signifikanten Sicherheitsvorfällen zwischen Januar und Juni 2022 zeigt, dass etwa zwei Drittel (67%) hauptsächlich Automobilzulieferer betrafen. Die komplexe Lieferkette gilt als große Schwachstelle und bietet zentrale Angriffspunkte, die mit hoher Wahrscheinlichkeit und oft großem Schadensausmaß ausgenutzt werden.

„Die Cybergefahrenlage für die Automobilbranche ist in den letzten Jahren kontinuierlich angestiegen. Mit der Verbreitung von Software-definierten Fahrzeugen, der Elektromobilität, dem autonomen Fahren und der vernetzten Lieferkette erhöhen sich die Cyber-Risiken weiter. Eine professionelle Cyber Security-Strategy von Unternehmen gewinnt als unerlässlicher Hygienefaktor in der Automobilindustrie stark an Bedeutung," erklärt Studienleiter Prof. Dr. Stefan Bratzel vom Center of Automotive Management (CAM). „Die Unternehmen unterscheiden sich jedoch bezüglich der Qualität von Konzeption und Umsetzung erheblich. Eine hohe Cyber Security Performance erhöht die Resilienz vor den zunehmenden Cyber-Angriffen und ermöglicht eine schnelle Erkennung und angemessene Reaktion auf entsprechende Vorfälle."

Connected Cars & Services führen zu mehr Angriffsvektoren

Kundenwünsche nach Connected Cars und Connected Services erzeugen einen enormen Wettbewerbsdruck, durch den Sicherheitsaspekte mitunter in den Hintergrund geraten. Zusätzlich ist die Umsetzung von Automotive Cyber Security sehr aufwendig: Sie umfasst den gesamten Produktlebenszyklus des Fahrzeugs von der Entwicklung über die Produktion bis hin zur Fahrzeugnutzung. Dabei muss die Sicherheit in einer komplexen

Wertschöpfungskette mit einer verteilten Verantwortung im großen Lieferanten- und Partnernetzwerk gesichert werden.

Dies fordern auch neue regulative Vorgaben zur Cybersicherheit in Kraftfahrzeugen wie die UN R155 (15) und die EU-Verordnung 2018/858. Sie müssen seit Juli 2022 von den Herstellern in der EU verpflichtend für alle neuen Fahrzeugtypen und ab Juli 2024 auch für alle bestehenden Fahrzeugtypen umgesetzt werden.

„Für Automotive-Unternehmen wird das Thema Cyber Security erfolgsentscheidend“, ergänzt Christian Korff, Managing Director Global Accounts und Mitglied der Geschäftsleitung von Cisco Deutschland und Auftraggeber der Studie. „Die Automobilindustrie ist ein Eckpfeiler unser deutschen Wirtschaft. Wir dürfen uns hier keine Anfälligkeiten im Cyberbereich erlauben. Nur wer auf allen ebenen sichere Fahrzeuge und Services bereitstellt, behält das Vertrauen der Kunden.“

Cyberangriffe steigen

Eine im Rahmen der Studie durchgeführte Meta-Analyse zu den Cyber-Angriffen auf Fahrzeuge und Unternehmen der Automobilwirtschaft offenbart die stark zunehmenden Risiken. Die Auswertungen der bisherigen Angriffspunkte auf die Cybersicherheit der internationalen Automobilwirtschaft zeigen, dass die Quantität und Qualität der Angriffe in den letzten Jahren erheblich gestiegen ist. Sie betreffen die gesamte Automobilindustrie, wie aktuelle Beispiele aus den Jahren 2022 und 2023 zeigen:

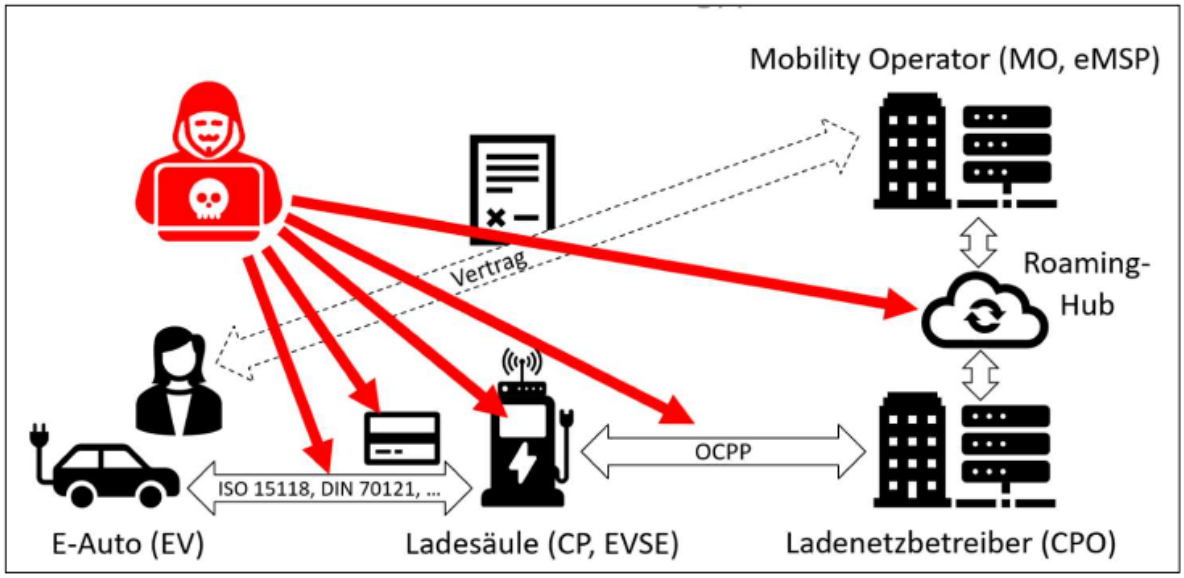
- Nachdem ein Zulieferer von Kunststoffteilen und elektronischen Komponenten von einem mutmaßlichen Cyber-Angriff getroffen wurde, musste Toyota im Februar 2022 den Betrieb seiner japanischen Fabriken kurzzeitig aussetzen und konnte rund 13.000 Autos nicht planmäßig bauen.
- Der US-Hersteller General Motors gab bekannt, dass er im April 2022 Opfer eines Cyber-Angriffs wurde, bei dem einige Kundendaten preisgegeben wurden und Hacker Prämienpunkte gegen Geschenkkarten einlösen konnten.
- Auch der Zulieferer Continental wurde zum Ziel von Cyberkriminellen. Eine Untersuchung des Vorfalls im Sommer 2022 hat ergeben, dass die Angreifer trotz etablierter Sicherheitsvorkehrungen einen Teilbestand an Daten aus betroffenen IT-Systemen entwenden konnten.
- Im März 2023 wurde von einem Cyber-Angriff auf Tesla berichtet, bei dem sich Hacker aus der Ferne in ein Fahrzeug einwählen und diverse Funktionen ausführen konnten. Dazu zählten etwa die Betätigung der Hupe, das Öffnen des Kofferraumes, das Einschalten des Abblendlichts sowie die Manipulation des Infotainment-Systems.
- Software-Schwachstellen in der multimodalen Mobilitäts-App Moovit führten im August 2023 dazu, dass Sicherheitsforscher zahlreiche Registrierungsdaten von verschiedenen Benutzerkonten abgreifen und für kostenfreie Fahrten ausnutzen konnten.

„Die Automobilbranche bietet auch durch die zunehmende Vernetzung viele Angriffsmöglichkeiten für professionelle Cyberangreifer - egal ob im Auto selbst, bei der Produktion oder den verzweigen Logistigketten,“ erklärt Holger Unterbrink, Technical Leader

bei Cisco Talos – einer der größten kommerziellen Threat Research Einheiten der Welt. „Angreifer gehen heute äußerst professionell vor. Sie suchen schlecht gesicherte Zugänge in komplexen IT-Umgebungen bei Unternehmen mit hoher Reputation und hohen Cash-Reserven. Da bietet die Automobilindustrie ein lohnenswertes Ziel. Ich erwarte hier in den nächsten Jahren eine weitere Zunahmen der Cyberattaken."

Die Studie hat in einem „Deep Dive" zur Elektromobilität herausgearbeitet, dass die Ladeinfrastruktur für Elektrofahrzeuge zu den besonders gefährdeten Bereichen zählt. Das Lade-Ökosystem ist durch seine verschiedenen Marktteilnehmer außerordentlich komplex und bietet grundsätzlich viele Angriffspunkte für Cyber-Kriminelle. Insgesamt zeigt die Analyse der Cyber-Angriffe, dass das Bewusstsein in der Branche für die Gefahren und Risiken noch deutlich unterentwickelt ist.

Abb. 16: Angriffsmöglichkeiten auf das E-Mobility-Ökosystem



Quelle: CAM/rt-solutions.de

Große Unterschiede beim Status

Das Erreichen einer hohen Cyber Security Performance in Automobilunternehmen erfordert somit große Anstrengungen und muss kontinuierlich überprüft werden. Die auf unterschiedlichen Wertschöpfungsebenen und -stufen der Branche verorteten Unternehmen unterscheiden sich dabei erheblich im Hinblick auf die Qualität der Konzeption und Umsetzung von Cybersicherheitsprogrammen. Sie befinden sich vor allem bei vielen Zulieferern und Dienstleistern noch auf einem niedrigen Niveau. Mit zunehmender Vernetzung und Automatisierung der Lieferkette erhöht sich jedoch die Angriffsfläche. Dabei kann sich Malware von den internen Systemen eines Zulieferers auf Dienstleister-Netzwerke und sogar Unternehmensnetzwerke der Automobilhersteller verbreiten.

In der Studie wird ein Modell zur empirischen Bewertung der Cyber Security Performance von Automobilunternehmen vorgeschlagen. Das 4C-Modell vereint dafür relevante Leistungskriterien von Cyber Security in vier Dimensionen: Kompetenzen (Competencies), Kooperationen (Cooperations), Kultur & Organisation (Culture & Organisation) sowie die

Cyber-Strategie (Cyber Strategy). Die Erfüllung der zugehörigen Kriterien stellt laut den Studienautoren eine wichtige Voraussetzung für eine hohe Leistungsqualität von Cyber Security und damit den langfristigen Erfolg der Unternehmen dar.

Über die Studie

Die Studie „Automotive Cyber Security“ wurde vom Center of Automotive Management (CAM) in Kooperation mit Cisco Systems verfasst. Methodisch beruht sie auf einer umfassenden Literaturanalyse von empirischen Studien zur Cyber Security in der Automobilbranche. Darüber hinaus wurden Expertengespräche mit hochrangigen Vertretern von Automobilherstellern, Zulieferunternehmen und Verbänden geführt sowie die Ergebnisse in Expertenworkshops reflektiert.

Über das CAM

Das Center of Automotive Management (CAM) ist ein unabhängiges, wissenschaftliches Institut für empirische Automobil- und Mobilitätsforschung sowie für strategische Beratung an der Fachhochschule der Wirtschaft (FHDW) in Bergisch Gladbach. Das CAM fokussiert seine Forschungen auf die Innovationstrends und Erfolgsfaktoren in den Zukunftsfeldern der Elektromobilität, des Software-definierten Fahrzeugs, des autonomen Fahrens und der Mobilitätsdienstleistungen. Auf Basis eines fundierten Branchen-Know-hows und umfangreicher Datenbanken, insbesondere zu fahrzeugtechnischen Innovationen der globalen Automobilindustrie sowie zu Mobility Services, erarbeitet das Auto-Institut individuelle Marktforschungskonzepte und praxisorientierte Lösungen für seine Kunden aus der Automobil- und Mobilitätswirtschaft.

Über Cisco

Cisco (NASDAQ: CSCO) ist das weltweit führende Technologie-Unternehmen, welches das Internet ermöglicht. Cisco eröffnet neue Möglichkeiten für Applikationen, die Datensicherheit, die Transformation der Infrastruktur sowie die Befähigung von Teams für eine globale und inklusive Zukunft. Weitere Informationen finden Sie unter: http://cs.co/presse.

https://emear.thecisconetwork.com/

http://gblogs.cisco.com/de

http://www.facebook.com/CiscoGermany

https://twitter.com/#!/cisco_germany

Sitz der Gesellschaft: Cisco Systems GmbH, Parkring 20, 85748 Garching, Amtsgericht München HRB 102605; WEEE-Reg.-Nr. DE 65286400