
## Thema

*Die zunehmende Vernetzung von Fahrzeugen untereinander, mit Smartphones und zentralen Infrastrukturen (Car2X) sowie Erweiterungen wie Unfalldatenschreiber und das System „eCall" wurden bisher in Bezug auf IT-Sicherheitsaspekte und Datenschutzbetrachtungen in der Automobilindustrie im Gegensatz zu Fragen der Functional- und Road-Safety niedriger priorisiert. Das Bewusstsein über die Gefahren, die durch mangelhafte IT-Sicherheit im Automotive-Umfeld ausgehen, hat sich durch die zahlreichen Incidents und Veröffentlichungen in 2015 spürbar verändert. Die Speicherung und der Austausch von Fahrzeug- und Bewegungsdaten wecken Begehrlichkeiten bei Industrie, Polizei und Justiz, Versicherungen und Dienstleistern aber auch bei Kriminellen. Und aus der Vernetzung und Steuerungsmöglichkeit von Fahrzeugen via Funk ergeben sich komplett neue Bedrohungsszenarien im Bereich der IT-Sicherheit mit Auswirkungen auf die Functional- und Road Safety.*

## Zielsetzung

Das halbtägige Seminar vermittelt in kompakter Form die IT-Sicherheitsgrundlagen welche spezifisch für den Automotive-Bereich relevant sind. Zu den Inhalten gehören insbesondere:

- Automotive-Innovationen wie Car2X und autonomes Fahren und damit verbundene IT-Sicherheitsrisiken und Schutzmaßnahmen
- Zusammenhang von Security und Safety
- Haftungs-, Datenschutz- und Privacy-Aspekte
- Bedeutung von Automotive-Forensic
- Top 10 Code of Conduct-Empfehlungen zu Datensicherheit, -hoheit und -zugriff

## Zielgruppe

Das Seminar richtet sich an Führungskräfte und Entscheider sowohl bei OEM als auch bei Zulieferern im Automotive-Bereich.

## Termine

Das ESG Cyber Training Center (CTC) bietet das Seminar in 2016 im CTC-Seminarprogramm (Termin wird demnächst auf der CTC-Webseite veröffentlicht) sowie auf Anfrage als Inhouse-Schulung bei Kunden vor Ort an.

# Automotive Security-Grundlagen für Führungskräfte

## INHALTE

**Einführung**

- Das moderne Auto fährt elektrisch, autonom und vernetzt
- Angriffsmöglichkeiten und Risiken
  - betroffene Systeme
  - Zusammenhang Safety und Security
  - Systeme und Aspekte in der Übersicht
- Gesellschaftliche und rechtliche Aspekte

**Risikofelder und Schutzmaßnahmen / Empfehlungen**

- Missbrauchsszenarien bei Car2X bzw. Vehicle2X
- Fahrzeugsteuerung – Eingriffe via Internet, Gateway-Attacken, Funk-Adapter und OBD
- Schwachstellen bei der Smartphone-Kopplung
- Angriffsszenarien auf Kfz-Systeme am Beispiel von Reifendruckkontrollsystemen und LIDAR
- Angriffe und Problematik by Pay-as-you-drive-Modulen und -Konzepten
- Angriff via Man-in-the-Middle-Attacke auf Automotive Telematik-Dienst
- Unfalldatenschreiber bzw. Datenschreiber für automatisiertes Fahren (Technik, Datenschutz und juristische Fragestellungen)
- eCall – Ungeklärte Aspekte bei Datenschutz, Tracking und forensischer Auswertung
- Angriffsszenarien auf Car-Sharing-Systeme

**Haftungs-, Datenschutz- und Privacy-Aspekte**

- BDSG und Datenschutz im Automotiv-Umfeld
- „Besitz“ von Daten
- Wiener Übereinkommen über den Straßenverkehr
- Verantwortlichkeit und Haftung im Kontext von automatisiertem Fahren
- Lifecycle und Qualitätssicherung
- Vorratsdatenspeicherung
- Regeln und Sicherheitsstandards beim Datenzugriff und Datenschutz
- Ethik und gesellschaftliche Akzeptanz

**Forensik im Automotive-Bereich – Zweck, Bedeutung, Möglichkeiten**

- Datensicherungs-Sichtweise
- IT-Sicherheits-Sichtweise
- Forensik-Sichtweise
- Grenzen von Penetrationstests und Reverse Engineering

**Zusammenfassung – Die Top 10-Empfehlungen für einen Code of Conduct bei Datensicherheit, -hoheit und -zugriff**

- Datensparsamkeit: So viel wie nötig und so wenig wie möglich
- Datenhoheit: Der Fahrer/Halter hat die Datenhoheit
- Datensicherheit: Anwendung etablierter IT-Sicherheitsprozesse
- Privacy by Design: Recht auf Anonymität
- Transparenz: Offener und ehrlicher Umgang mit Daten
- Fairer Interessenausgleich: Abwägung von Chancen und Risiken
- eCall: Kein Tracking und kein UDS über die Hintertür
- Standards: Hersteller- und länderübergreifende Verständigung
- Recht: Klarstellungen und Präzisierungen
- Forensic-Readiness: Log or not

## Referent

**Dipl.-Ing. Thomas Käfer**, M.Sc. ist öffentlich bestellter und vereidigter Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung und Geschäftsführer eines eigenen IT-Systemhauses. Seit 1990 befasst er sich mit IT-Sicherheit und digitaler Forensik und seit 2012 mit Schwerpunkt im Bereich Automotive Security und Car Forensics.

Herr Käfer hat den Master-Studiengang „Digitale Forensik“ mit der Forschungsarbeit zum Thema Digitale Kfz-Forensik erfolgreich abgeschlossen.