Security in vernetzten Fahrzeugen

Für Connected Cars ergeben sich aus der Kommunikation zwischen Fahrzeugen und mit der Infrastruktur und Service-Providern viele neue Anwendungspotenziale, aber auch Risiken z. B. im Hinblick auf IT-Sicherheit. Die ESG arbeitet daran, die Lücke der Automotive Domäne gegenüber der klassischen IT-Branche bezüglich der systemspezifischen Definition und praktischen Anwendung von Security-Prozessen und -Standards zu schließen.

Die Automobilindustrie verfolgt seit einigen Jahren auf unterschiedlichen Ebenen sehr aktiv das Ziel einer vernetzten Fahrzeuglandschaft. Ein Ende dieses Trends wird nicht erwartet, sondern im Gegenteil eine immer höhere Zahl an Connected Cars und eine immer stärkere digitale Verknüpfung zwischen Fahrzeugen, Nutzern, OEMs, Zulieferern und IT-Dienstleistern. Dies zeigt Bild 1 als Teilergebnis einer Studie zum Thema Innovation & Security for Connected Cars. Für diese 2014 durchgeführte Studie wurden über 300 Experten und Entscheidungsträger aus dem Automotive-Bereich, der IT-Branche und von Telekommunikationsunternehmen zu den Themen Connectivity, Datenmanagement, IT-Sicherheit und gesetzlichen Rahmenbedingungen befragt.

Die Studie bestätigt, dass im Umfeld der Connected Cars insbesondere die Security-relevanten Fragestellungen für vernetzte Systeme weder vollumfänglich definiert, geschweige denn beantwortet sind. Vor allem in den Bereichen der technischen Beherrschbarkeit von Security-Aspekten, der gesetzlichen Regelungen zum Umgang mit digitalen Daten sowie der Nutzerakzeptanz von datenbasierten Fahrerassistenzsystemen sind noch Hürden zu meistern (siehe Bild 2). Darüber hinaus sind auch noch nicht alle Rollen in der Wertschöpfungskette verteilt und entsprechende Business-Modelle definiert. Eine wichtige Frage, die in diesem Zusammenhang beantwortet werden muss, ist: Wer erhält Zugriff auf welche Daten? Diese Information ist für die beteiligten Unternehmen ein zentraler Bestandteil zur Definition ihres Leistungsportfolios.

Daten und Kommunikation

Die zentralen Elemente dieser vernetzen Systeme sind die digitalen Daten und die digitale Kommunikation, die in vielerlei Hinsicht einen hohen Wert sowohl für den Dienstanbieter als auch für den Nutzer haben. Die Nutzer generieren durch ihr Verhalten einen Großteil der Daten, die für Connected-Car-Anwendungen benötigt werden. Deswegen ist der einzelne Nutzer daran interessiert, dass seine persönlichen Daten geschützt und nur entsprechend seiner Zustimmung verwendet werden. Die Dienstanbieter sind an der Sicherheit der Daten interessiert, da diese notwendig für die angebotenen Dienste sind und eine Beeinträchtigung der Sicherheit unter Umständen einschränkende funktionale Auswirkungen sowie rechtliche und wirtschaftliche Folgen nach sich zieht. Insbesondere die Gewährleistung der Privacy, also der Schutz der Privatsphäre, von Nutzerdaten wird zunehmend auch gesetzlich verlangt.

Alle Bilder: ESG

In der klassischen IT-Branche wird Security bereits seit Längerem aktiv gelebt. Es gibt zahlreiche Standards, Normen und Vorschriften, welche nicht nur die vier Säulen der IT-Security (Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität) betrachten, sondern auch die verschiedenen Ebenen im Entwicklungsprozess einschließen. Hier sind z. B. Standards und Prozesse der Informationssicherheits-Managementsysteme (ISMS) wie der ISO-27000-Familie und dem Grundschutz Handbuch zu erwähnen, aber auch Methoden zur Evaluierung von IT-Sicherheit wie zum Beispiel in den Common Criteria (ISO/IEC 15408). Während die IT-Security hier bereits mit viel Erfahrung gelebt wird, so gibt es wenig praktische Erfahrung mit einer branchenspezifischen Umsetzung im Bereich der Connected-Car-Plattformen.

Bei der Firma ESG werden Security Ansätze entwickelt und praktisch eingesetzt, welche speziell auf den Einsatz in der Welt der vernetzen Fahrzeuge zugeschnitten sind. Hierzu wurde zunächst eine Reihe von Security Standards und Prozessen untersucht und in Bezug auf eine branchenspezifische Anwendung evaluiert. Insbesondere wurden für Automotive und ebenso für den Einsatz im militärischen Bereich die folgenden Standards als notwendig und besonders zielführend eingestuft:

- ISO/IEC-27000-Familie: Die ISO/IEC-27000-Reihe ist eine Reihe von Standards der IT-Sicherheit, bestehend aus über 20 Normen (Stand: Juni 2013). Enthalten sind u. a. Begriffsdefinitionen, Anforderungen an ein ISMS, Empfehlungen für diverse Kontrollmechanismen, IS Risikomanagement, Zertifizierungsvorschriften sowie Leitfaden für Auditoren zur ISO-27000-Zertifizierung.
- BSI-Grundschutzhandbuch und -katalog: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet das IT-Grundschutzhandbuch (GSHB) an, welches detailliert IT-Sicherheitsmaßnahmen aus verschiedenen Bereichen (Technik, Organisation, Infrastruktur und Personal) sowie Anforderungen an das IT-Sicherheitsmanagement beschreibt.
- ISO/IEC 15408 (Common Criteria): Für die Evaluierung und Zertifizierung von IT-Produkten und -systemen existiert der Standard ISO/IEC 15408 (Common Criteria). Neben einem Katalog vordefinierter Funktionalitäten legen die CC Anforderungen an die Vertrauenswürdigkeit gemäß einer Vertrauenswürdigkeitsstufe fest. Die CC bieten die Möglichkeit, Sicherheitsanforderungen in vorevaluierten Schutzprofilen zusammenzufassen.
- Cobit: Die Cobit umfasst eine Sammlung international akzeptierter und allgemein einsetzbarer Kontrollziele. Diese repräsentieren drei Sichten auf die IT und stellen die Interessen der jeweiligen Gruppe und deren Ziele dar. Sie umfassen folgende Aspekte:
  - Managementsicht: Unterstützung bei der Risikobehandlung in der sich ständig ändernden Umgebung und bei der Entscheidung über Investitionen, die zur Gestaltung der Kontrolle nötig sind,
  - Anwendersicht: Kontrolle und Sicherheit der Informatikdienstleistungen, »

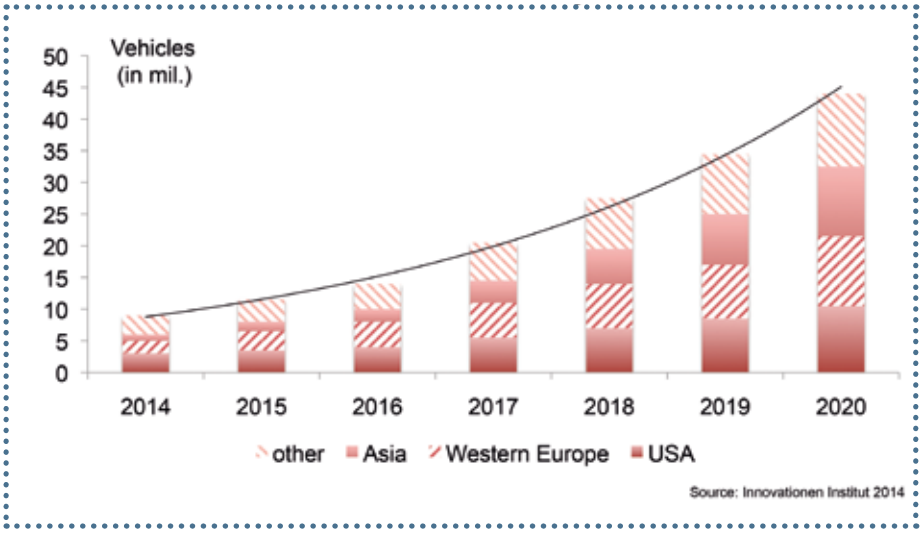

Bild 1: Erwartete Entwicklung der Verkaufszahlen von vernetzten Fahrzeugen.

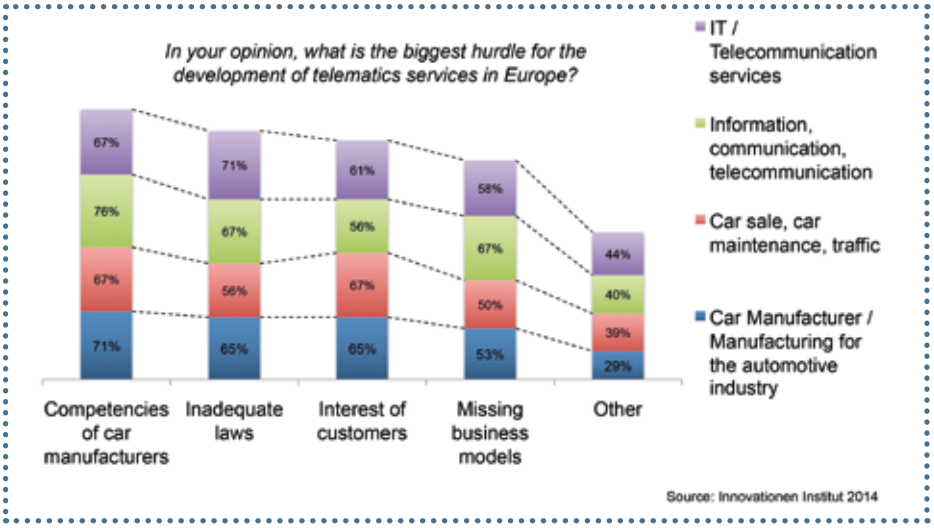

Bild 2: Hürden, die u. a. in Europa noch zu meistern sind.

Bild 3: Relevante Prozessschritte für eine Security-Analyse.

- Revisionssicht: Einheitliche Grundlage für die Wertung der inneren Kontrollen.
- ETSI TS 102 165 TVRA: Diese Spezifikation der European Telecommunications Standards Institute (ETSI) mit dem Titel „Technical Specification Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols" definiert Methoden zur Evaluierung und Analyse von Bedrohungen, Risiken und Schwachstellen der neuen Telekommunikationsnetzwerke. Sie besteht aus zwei Teilen: der erste Teil beschäftigt sich mit Methoden und Richtlinien für die Analyse von Bedrohungen, Risiken und Schwachstellen; der zweite Teil mit Sicherheitsmaßnahmen.
- ZDv 54/100: Die 4. ZDv 54/100 ist die Grundsatzvorschrift für die IT-Sicherheit im Geschäftsbereich des Bundesministeriums der Verteidigung (BMVg). Sie legt auf der Grundlage der IT-Strategie des BMVg (IT-Strategie BMVg, Anlage 13, Nr. 14) die Grundsätze für die Herstellung, Überwachung und Gewährleistung der IT-Sicherheit fest.

Aus diesen Standards wurden die grundlegenden Definitionen, Prozesse und Methoden untersucht und Gemeinsamkeiten sowie Unterschiede herausgearbeitet. Als ein Ergebnis daraus entstand der Ansatz für einen standardübergreifenden, in der Praxis anwendbaren Prozess zur Security-Analyse (Bild 3). Dieser kann vor allem zur Analyse technischer Schwächen und Bedrohungen eingesetzt werden.

Bedrohungsanalyse

Im Rahmen der Bedrohungsanalyse werden zunächst Assets definiert. Assets sind Elemente innerhalb des Systems, für die ein besonderer Schutzbedarf besteht. Vom speziellen Datensatz bis zur Hardware-Komponente gibt es hier bewusst keine Einschränkung. Über die Definition von Schwächen im System ergeben sich die Bedrohungen für die Assets. Daraus lassen sich mögliche Angriffe auf die Assets ableiten, die die Schwächen auszunutzen versuchen.

In der folgenden Design-Phase werden auf Basis der Ergebnisse der Bedrohungsanalyse Risiken für Angriffe/Bedrohungen ermittelt. Erst auf Basis dieser Risikowerte lassen sich Maßnahmen identifizieren, die die Sicherheit im System zielorientiert erhöhen.

Ein wichtiger Aspekt bei der Security-Analyse ist der Umstand, dass selbst bei korrekter und umfassender Umsetzung des Prozesses der Sicherheitsgewinn nur eine relative Verbesserung darstellen kann. Deshalb ist die Analyse und Ermittlung des Restrisikos nach Umsetzung von Gegenmaßnahmen notwendig, um das weitere Vorgehen darauf abstimmen zu können (z. B. Iteration des Prozesses). Es gibt Ansätze zur quantitativ messbaren Einschätzung des Restrisikos, die aber aufgrund von unerwartet eintretender und nicht berücksichtigter Angriffe an Aussagekraft verlieren. Belastbar bleibt dann nur eine qualitative Einschätzung gegenüber dem ungeschützten, nicht analysierten System.

Die einzelnen Schritte des generischen Prozesses lassen sich so je nach vorliegendem Projekt mit den Methoden aus den oben beschriebenen Standards und Normen durchführen. So wird sichergestellt, dass die Analyse möglichst nah am bestehenden, bewährten Standard erfolgt, aber auch an den Stellen sinnvoll ergänzt wird, an denen sich Lücken in den Standards auftun.

Fazit

Für die Welt der Connected Cars wurden konkrete automotive-spezifische Beispiele ausgewählt, an denen das oben beschriebene Vorgehen praktisch zur Umsetzung gebracht worden ist. Darüber hinaus ergaben sich durch die Anwendung in den weiteren ESG-Divisionen Avionik und militärische Landsysteme Synergien. So konnte die ESG diese Prozesse als Bestandteil der Unternehmensstruktur etablieren, um sie bereichsübergreifend in Projekten mit Bezug zur IT-Security einsetzen zu können. ■ (oe)

» www.esg.de

Dr. Michael Beimforde ist Senior System Engineer, Funktions- und Embedded-Software-Entwicklung in der Automotive Division bei der ESG Elektroniksystem- und Logistik-GmbH.

Manuel Bernard ist Senior System Engineer, Funktions- und Embedded-Software-Entwicklung in der Automotive Division bei der ESG Elektroniksystem- und Logistik-GmbH.