Standpunkt

IT-Sicherheit im Vernetzten Auto

Elektronische Datenverarbeitung ist häufig das Ziel krimineller Angriffe und Manipulationen. Das gilt umso mehr, wenn das Zielsystem – hier das Auto – vernetzt ist.

Hintergrund

In den letzten Jahren wurden durch IT-Sicherheitsexperten mehrere spektakuläre „Hacker-Angriffe“ auf Fahrzeuge durchgeführt und veröffentlicht, um auf das Risiko mangelhafter Absicherung der Fahrzeug-IT aufmerksam zu machen. Im Fokus stand dabei meist der Zugriff auf sicherheitskritische Funktionen der Fahrzeugsteuerung (Bremse, Lenkung) über eine unzureichend abgesicherte Funkschnittstelle.

Risiken

Prinzipiell kann jede unzureichend geschützte kabellose oder andere Datenschnittstelle eines Fahr-zeugs Einfallstor für einen Angriff sein. Bei vernetzten Fahrzeugen kommen noch die Smartphones der Eigentümer und die Rechenzentren der Hersteller und Dritter dazu, die ebenfalls angegriffen werden können.
Kriminelle Motive hinter Hacker-Angriffen können z. B. sein:

- Manipulation von Fahrleistung und Fahrzeugfunktionen (z. B. Chip-Tuning)
- Urkundenfälschung und Betrug (z. B. Tachobetrug)
- Fahrzeugdiebstahl und Fahrzeugeinbrüche ohne Gewaltanwendung
- Überwachung, Ausforschung, Spionage
- Erpressung, Bedrohung, Vandalismus, Terrorismus

Herausforderungen

Entwicklungszyklen und Lebenserwartung von Kfz sind deutlich länger als in der Informations- und Kommunikationstechnologie. Bereits zum Produktionsstart eines Fahrzeugs entsprechen die Informationstechnologien oftmals nicht mehr dem aktuellen Stand der Technik. Ähnlich wie in der Unterhaltungselektronik beginnen die Kfz-Hersteller, Software nachträglich zu aktualisieren, um Fehler zu beheben, Eigenschaften des Fahrzeugs zu optimieren und neue Funktionen zur Verfügung zu stellen. Dabei gilt es einige Herausforderungen zu meistern:

- Durch die Aktualisierung von Software und Hardware dürfen zulassungsrelevante Eigenschaften eines Fahrzeugs nicht unzulässig verändert werden.
- Im Zuge des Aktualisierungsprozesses darf keine Schadsoftware auf das Fahrzeug übertragen werden.
- Die fehlerhafte oder unvollständige Aktualisierung von Software darf nicht zu einem gefährlichen Zustand des Fahrzeugs führen.
- Heutige Kfz enthalten je nach Ausstattungsumfang zahlreiche Steuergeräte mit jeweils eigener Software. Die Kompatibilität unterschiedlicher Konfigurations- und Versionsstände muss gewährleistet sein.

ADAC Position

Der ADAC fordert den Nachweis einer zeitgemäßen Absicherung der Fahrzeug-IT gegen Angriffe und Manipulationen für die Typgenehmigung. Diese lässt sich systematisch konstruieren gemäß international zertifizierten Prozessen wie Common Criteria (ISO/IEC 15408). Die Eigenzertifizierung der Fahrzeughersteller selbst wird abgelehnt.
Die Datenkommunikation mit den IT-Systemen im Fahrzeug muss verschlüsselt über eine sichere Kommunikationsschnittstelle erfolgen.
Der Fahrzeughersteller muss über die Lebensdauer des Fahrzeugs sicherheitsrelevante Software-Aktualisierungen zur Verfügung stellen und, sofern technisch notwendig, auch die erforderliche Anpassung der Hardware anbieten. Fahrzeughalter müssen darauf vertrauen können, dass sie ihr Fahrzeug dauerhaft nutzen können.