title krone.at
issue 19/04/2021
page Online

SOFTWARE IM AUTO

Rollende Schwachstellen: Hersteller unter Zugzwang

(Bild: ©Tierney - stock.adobe.com)

Mit dem Trend zu vernetzten Fahrzeugen gehen neue Bedrohungsszenarien einher. Die Palette reicht vom Autodiebstahl durch die Manipulation der elektronischen Schließsysteme bis zur kompletten Fernsteuerung mit fatalen Auswirkungen. Neue Richtlinien bringen die Hersteller und Zulieferer im Hinblick auf die Cyber-Sicherheit nun unter Zugzwang.

Ab Juli 2022 müssen alle neu typgenehmigten Fahrzeuge entsprechende Risiken vom Beginn der Entwicklung an berücksichtigen, wenn sie in der EU oder auch in Japan zugelassen werden wollen, erklärte Willibald Krenn vom AIT Austrian Institute of Technology im Gespräch mit APA-Science. Die Standardisierungsgremien und Regulierer hätten damit auf den deutlichen Anstieg bei den Bedrohungen und publik gewordenen Schwachstellen reagiert.

Angriffsflächen werden größer

Handlungsbedarf scheint jedenfalls gegeben: „Fahrzeuge haben inzwischen viele Wireless-

Features. Und die Konnektivität wird noch deutlich zunehmen, wenn das Auto mit anderen Verkehrsteilnehmern oder der Infrastruktur, beispielsweise Ampeln, kommuniziert. Das sind Angriffsflächen, die man mitdenken muss", so der Experte. Attacken könnten aber auch über herkömmliche Wege analog zum Internet erfolgen. Eine Handy-App, mit der man gewisse Funktionen im Fahrzeug steuern kann, reiche möglicherweise schon aus, dass Kriminelle einen Weg ins Auto finden.

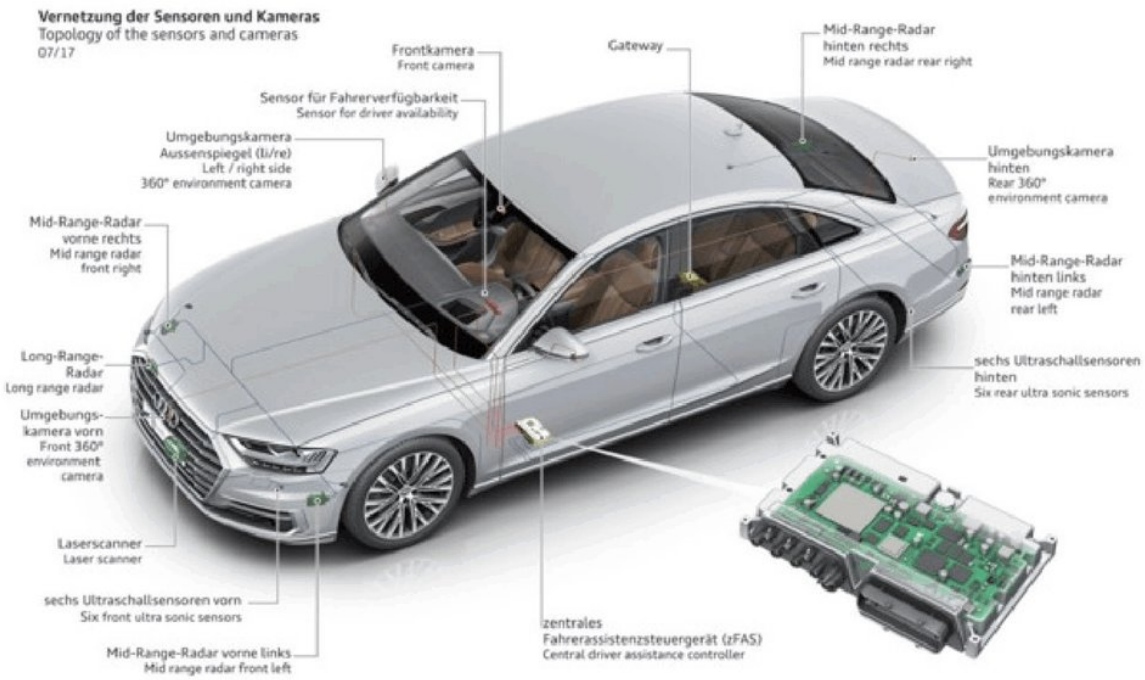
Hacker haben sich Krenn zufolge schon die Bordcomputer näher „angesehen". „Sie fanden darin eine SIM-Karte, haben sie in einen Laptop eingebaut und es geschafft, sich über diese Telematikverbindung bei den Anbietern einzuschleichen." In Indien wiederum seien Tausende Fahrzeuge gestohlen worden, nachdem Angreifer eine Schwachstelle im Steuerungssystem entdeckt haben. So konnten sie die Autos aufsperren, den Motor starten und wegfahren. „Cybersicherheit entwickelt sich zum zentralen Thema, mit dem sich die Industrie beschäftigen muss", ist Krenn überzeugt.

(Bild: ©scharfsinn86 - stock.adobe.com)

Lebensgefahr durch manipulierte Bremsen

Lebensgefährlich wird es, wenn Fahrzeuge ferngesteuert oder relevante Funktionen torpediert werden. „Forscher haben beispielsweise herausgefunden, dass man eingebaute Fahrassistenzsysteme, die oft kamerabasiert sind, manipulieren kann. Durch das Projizieren eines virtuellen Verkehrszeichens in das 'Gesichtsfeld' der Kamera wird dem Fahrzeug etwa ein Stopp-Schild vorgetäuscht. Auf der Autobahn ist das sicher extrem problematisch", erläuterte der Experte des Center for Digital Safety & Security. Theoretisch könnten Hacker das Auto auch in den Gegenverkehr steuern oder überraschend für den Nachkommenden eine Notbremsung einleiten.

Neue europäische Sicherheitsrichtlinien verpflichten nun die Hersteller, die Cybersicherheit ihrer Fahrzeugsysteme nachweislich zu überprüfen, um eine Zulassung zu erhalten. Im Rahmen einer Risikobeurteilung müssen mögliche Bedrohungspotenziale identifiziert und dokumentiert sowie erkannte Probleme gelöst werden - und das schon von der Designphase weg. Genau das soll ein Werkzeug namens THREATGET ermöglichen, das am AIT gemeinsam mit LieberLieber Software entwickelt wurde. „Dieses Management-Tool wird in den Engineering-Lifecycle eingebettet und hilft dabei, ein cybersicheres Design zu erarbeiten", so Krenn.



Die Vernetzung der Sensoren und Kameras(Bild: Audi)

Sicherheit vom Reißbrett weg

Wird ein Fahrzeug oder ein Teilsystem am Reißbrett entworfen, kann man damit die einzelnen Komponenten modellieren und festlegen, welche Sicherheitseigenschaften sie haben. „Also etwa, dass beispielsweise ein Computer mit der Bremse und einer Kamera sowie einem bestimmten Datenaustauschsystem verbunden ist. Wenn der Entwurf fertig ist, führt das Tool eine Analyse bezüglich Cybersicherheit durch und vergleicht das Modell mit schon bekannten Schwachstellen und schlechten Designs", erklärte der Experte. Das System zeige potenzielle Gefahren auf und gebe teilweise auch Empfehlungen, was besser gemacht werden könnte.

„Die Problemfelder wird man sich ansehen und redesignen oder die Sicherheitseinstellungen entsprechend nachschärfen, etwa indem man bei der Datenübertragung auf Verschlüsselung statt eine Prüfsumme setzt. Im Modell lässt sich das einfach ein- und ausschalten, wobei die Auswirkung gleich ersichtlich ist", sagte Krenn. Sobald neue Schwachstellen publik werden, landen sie in einer Bedrohungsdatenbank. Diese wird zum Teil in Handarbeit von Fachleuten befüllt, aber auch eine künstliche Intelligenz fischt neue Informationen aus bestehenden Quellen heraus. „Das ist aktuell unsere Forschungsstoßrichtung bei THREATGET", so der Fachmann. Dann beginnt die nächste Runde: Das analysierte Modell wird erneut unter die Lupe genommen und aktualisiert - Sicherheit geht schließlich vor.

krone.at