# „Harmonisches Zusammenspiel"

## Dr. Thomas Wollinger über holistische Security fürs vernetzte Fahrzeug

Die Automobilbranche befindet sich im Umbruch. Automotive Security wird zum kritischen Erfolgsfaktor. Im Interview erläutert Dr. Thomas Wollinger, Geschäftsführer der ESCRYPT GmbH, wie Denken und Handeln hier gerade die Richtung ändern – und warum es dafür einen Dirigenten braucht.

**Herr Dr. Wollinger, vollzieht sich in der Automobilbranche gerade ein Bewusstseinswandel im Hinblick auf das Thema Security?**

**Dr. Thomas Wollinger:** Die Entwicklung hier ist tatsächlich sehr spannend. Die Branche steht ja insgesamt vor einem fundamentalen Wandel – bis hin zu gänzlich neuen Geschäftsmodellen, die künftig weniger auf dem Verkauf von Autos, sondern mehr auf datengetriebenen Services beruhen. Die zunehmende Digitalisierung und Konnektivität haben den Abschied von traditionellen Fahrzeugplattformen mit statischen Steuergeräten hin zu Ethernet-basierten Plattformen mit verteilten und vernetzten ECUs längst eingeläutet. Da werden einzelne eingebettete Security-Funktionen allein nicht mehr ausreichen. Man muss über das Fahrzeug hinaus denken und handeln – holistisch eben.

**Wie meinen Sie das?**

**Dr. Thomas Wollinger:** Wenn wir über die Zukunft sprechen, reden wir über vernetztes und autonomes Fahren. Und das beruht auf Echtzeitdatenaustausch. Die Angriffsfläche erweitert sich dadurch enorm und die Bedrohung bekommt eine ganz neue Dimension. Denn wenn Fahrzeuge zu rollenden Computern im Netz werden, wird IT-Sicherheit zu einer Frage der persönlichen Sicherheit.

Das „System Auto" muss daher komplett abgesichert werden, aber auch die Kommunikation der Fahrzeuge untereinander und mit Verkehrsanlagen und auch die Verkehrsinfrastruktur selbst. Und das über den gesamten Lebenszyklus hinweg. Fahrzeuge, die 15 Jahre oder länger auf der Straße sind, müssen wir vor Cyberangriffstechniken schützen können, die wir heute noch gar nicht kennen. Und dafür müssen wir beizeiten die nötigen Prozesse und die notwendige Organisation vorhalten. „Holistic Automotive Security", wie wir sie bei ESCRYPT verstehen, benötigt also eine wirksame Absicherung des gesamten Systems und seiner Infrastruktur, und zwar dauerhaft über den gesamten Lebenszyklus hinweg und mit einer Organisation dahinter, die genau das ermöglicht.

**So weit die graue Theorie. Wie soll das in der Praxis aussehen?**

**Dr. Thomas Wollinger:** Ein gutes Beispiel ist unsere Intrusion Detection and Prevention Solution: Dabei überwacht Security-Software im Fahrzeug die zentralen Steuergeräte und Gateways. Anomalien in der Bordnetzkommunikation werden erkannt, dokumentiert und an ein Security Operations Center im Backend weitergeleitet. Dort werden die aggregierten Daten über Analysetools ausgewertet und bei Cyberattacken gemäß festgelegter „Incident Response Procedures" Security-Updates an die gesamte Fahrzeugflotte ausgebracht. Der große Vorteil: Neue Angriffsmuster werden bereits erkannt, sobald sie einzelne Fahrzeuge treffen und münden direkt in Schutzmaßnahmen für die gesamte Flotte. Es entsteht eine Art Immunsystem, in dem die IT-Sicherheitsmechanismen über den gesamten Lebenszyklus nachhaltig gepflegt werden und organisatorisch unterfüttert sind.

**Das heißt, die IT-Sicherheit ihrer Fahrzeugflotten hängt für die Autobauer nicht nur von den Security-Maßnahmen selbst, sondern vielmehr auch von deren Koordination und Management ab?!**

**Dr. Thomas Wollinger:** Völlig richtig. Die Absicherung ihrer Fahrzeugflotten wird für die OEMs zu einer andauernden komplexen Aufgabe von hoher Wichtigkeit. Sie benötigen hier vorausschauende Konzepte, feste Security-Strukturen und ausreichende Ressourcen. Und sie benötigen ein zentrales Security-Management, das ein harmonisches Zusammenspiel aller Security-Maßnahmen sicherstellt und alle Beteiligten beim OEM selbst, aber auch externe Dienstleister, Zulieferer und Werkstätten durchtaktet. Ähnlich einem Dirigenten, der ein Orchester führt und entwickelt.

So wie die Autohersteller heute schon die Prozesse und Anforderungen ihres Kerngeschäfts orchestrieren, müssen sie künftig auch die Automotive Security orchestrieren. Denn der Weg zur Smart Mobility führt nur über wirksame IT-Sicherheit. ■


Dr. Thomas Wollinger,
Geschäftsführer ESCRYPT GmbH

„Wenn Fahrzeuge zu rollenden Computern im Netz werden, wird IT-Sicherheit zu einer Frage der persönlichen Sicherheit."