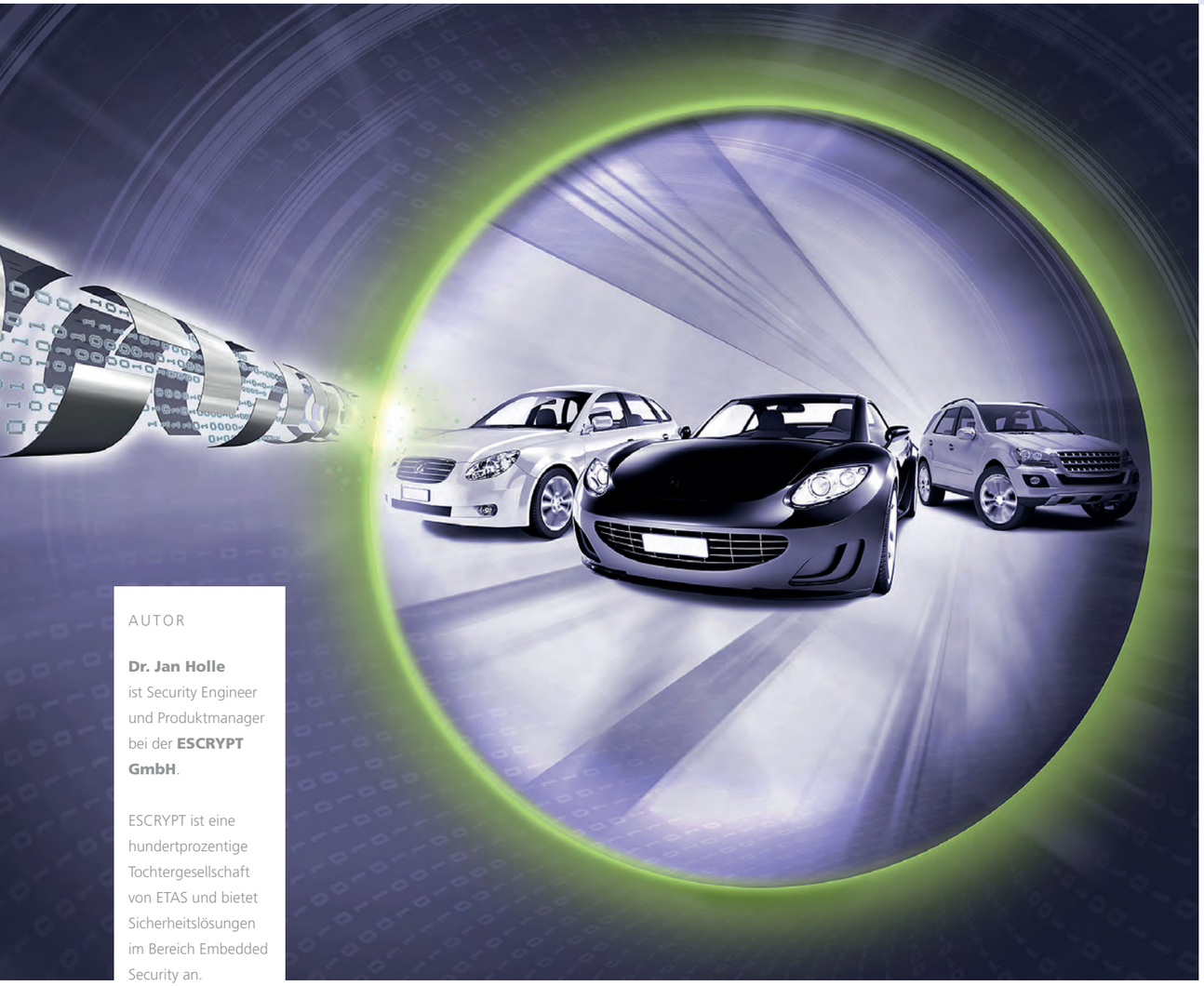
Immunsystem für das vernetzte Fahrzeug

Schutz durch Intrusion Detection and Prevention System (IDPS)

Mehr Sicherheit und Komfort. Optimierter Service und kurzweiligere Autofahrten. Die Liste der Vorteile von vernetzten Fahrzeugen ist lang. Doch die Einbindung ins Internet der Dinge birgt auch Risiken. So steigt die Gefahr von Cyber-Attacken. Angreifer finden immer neue Angriffspunkte. Darum brauchen vernetzte Fahrzeuge lernende Abwehrsysteme. Diese erkennen Angriffe auch dann, wenn das Muster noch unbekannt ist und können neue Erfahrungen zügig an andere Fahrzeuge im Feld weitergeben.



AUTOR

Dr. Jan Holle ist Security Engineer und Produktmanager bei der **ESCRYPT GmbH**.

ESCRYPT ist eine hundertprozentige Tochtergesellschaft von ETAS und bietet Sicherheitslösungen im Bereich Embedded Security an.

Sind Fahrzeuge in Kundenhand, dann haben Hersteller nur punktuell Zugriff auf deren Systeme. Dennoch erwarten Käufer zurecht, dass ihre Fahrzeuge jederzeit sicher sind. In Zeiten zunehmend vernetzter Fahrzeuge tut sich damit eine neue Herausforderung auf. Zwar erhalten die Hersteller bessere Zugriffsmöglichkeiten, doch steigt mit der Einbindung ins Internet der Dinge auch das Risiko unbefugter Zugriffe und böswilliger Cyber-Attacken.

Funktionale Sicherheit (Safety) allein reicht nicht mehr. Hersteller müssen auch umfassende IT-Sicherheit (Automotive Security) garantieren, wenn hunderte Millionen vernetzte Fahrzeuge in aller Welt unterwegs sind. Hinzukommt der Trend zum automatisierten Fahren, der die Sicherheitsanforderungen an IT-Systeme weiter erhöht.

Holistischer Schutz über den Gesamtlebenszyklus hinweg

Um das nötige Sicherheitsniveau zu erreichen, bedarf es durchdachter und sauber implementierter Maßnahmen. Automotive Security ist nicht – oder nur zu horrenden Kosten – nachrüstbar. Gefragt sind vielmehr holistische Strategien, in denen Safety und Security von Tag eins der Entwicklung an zusammen betrachtet werden. Standardisierte Prozesse in der Entwicklung von Embedded Software gehören ebenso dazu wie zuverlässige Schutzvorkehrungen. Moderne Chip-Architekturen mit Hardware-Security-Erweiterungen – darunter Hardware-Security-Module und Secure-Hardware-Extensions – schirmen sicherheitsrelevante Systembereiche physikalisch gegen unbefugte Zugriffe ab. Rund um diese Sicherheitskerne sind weitere Maßnahmen nötig: Secure-Boot-Funktionen, die etwaige Manipulationen an der Steuergeräte-Firmware erkennen, sowie geschützte Netzwerkübergänge (Gateways) oder kryptografische Lösungen zur Absicherung sämtlicher Kommunikation. Nicht minder wichtig sind organisatorische Schutzmaßnahmen in der Entwicklung und Produktion, von zugangsbeschränkten Sicherheitsbereichen bis hin zur Begrenzung der Zugriffsrechte auf Krypto-Schlüssel und Freischaltcodes auf einige wenige Verantwortliche. Die beschriebenen Maßnahmen senken die Wahrscheinlichkeit von zufälligen Fehlern. Und sie erhöhen den Aufwand für Hacker, in Fahrzeugsysteme einzudringen. Doch sie beantworten noch nicht die Frage, wie der Schutz vernetzter Systeme zu gewährleisten ist, sobald das Fahrzeug in Kundenhand ist. Denn in dieser Kernphase des Lebenszyklus bleiben die Zugriffsmöglichkeiten für Hersteller begrenzt. Sie müssen die Fahrzeugsysteme theoretisch während der Entwicklung für Angriffe wappnen, die über ein Jahrzehnt in der Zukunft liegen können. Ein Rückblick auf den Stand der Informationstechnologie vor zehn Jahren genügt, um zu verstehen, dass dies kaum möglich sein wird.

Die Herausforderung: Schutz vor unbekannten Gefahren

Daraus folgt: Die Maßnahmen der IT-Sicherheit müssen dynamisch und fortlaufend sein, um die Systeme auch in Kundenhand zuverlässig zu schützen. Doch während die Randbedingungen der funktionalen Sicherheit meist auf Naturgesetzen und statistischen Vorhersagen beruhen, die im Betrieb weiter gelten, sind die Annahmen und Randbedingungen der IT-Sicherheit volatil. Denn Angreifer suchen immer neue Schwachstellen im System. Es liegt in der Natur der Sache, dass die Hersteller in der Regel nicht um die Existenz dieser Schwachstellen wissen. Ebenso wenig können Security-Experten alle Angriffsstrategien vorhersehen, die viele Jahre in der Zukunft liegen. Auch die klassische IT steht vor der Aufgabe, IT-Infrastrukturen vor An-

griffen mit unbekanntem Muster zu schützen. Hier versuchen Angreifer, Sicherheitsmechanismen auszuhebeln, die als sicher gelten.
Schutz bieten hier immer öfter sogenannte intelligente Angriffserkennungs- und Abwehrsysteme (Intrusion Detection and Prevention Systems, IDPS). Bei näherer Betrachtung erscheinen diese Systeme dafür prädestiniert, auch das vernetzte Fahrzeug zu schützen.

Immunisierung per IDPS

Das Besondere an der IDPS-Technologie: Sie nutzt die Vernetzung der Fahrzeuge, um schnell auf neue Angriffsszenarien reagieren zu können und um die daraus resultierenden Abwehrstrategien umgehend an die gesamte Fahrzeugflotte weiterzugeben. So entsteht eine Art Immunsystem, das dynamisch auf Angriffe reagiert – und in dem jeder Angriff die Abwehrkräfte der Flotte stärkt. Kern des IDPS von ESCRYPT ist eine spezielle Security-Software. Sie wacht in Steuergeräten oder Gateways und analysiert permanent die komplette Bordnetzkommunikation. Tauchen Anomalien auf, dokumentiert sie diese – und leitet im Ernstfall die Abwehr ein. Ist das erkannte Angriffsmuster schon bekannt, blockieren Firewall-Mechanismen die Kommunikation zwischen den verschiedenen Datenbussen. Dies ist bereits Routine – und wie das gesamte IDPS auf heute gängige CAN- sowie auf künftige Ethernet-Netzwerke anwendbar. Die IDPS-Technologie ist aber vor allem in der Lage, unbekannte Muster und Angriffsstrategien zu erkennen und zu parieren. Dafür verfügt sie über hinterlegte Regelsets (Black-/Whitelists), die ständig aktualisiert werden. Genau hier liegt eine Stärke des Ansatzes: Anomalien und Anzeichen für bisher noch unbekannte Attacken werden von der Angriffserkennungssoftware CycurIDS detektiert. Sie kann erkannte Anomalien im Fahrzeug speichern, damit sie später auslesbar sind. Wirksamer ist aber eine Funktion, die alle Anomalien automatisch in eine cloudbasierte Eventdatenbank übermittelt. Hier laufen sämtliche Auffälligkeiten aus allen vernetzten Fahrzeugen des Herstellers mit den Fingerprints bekannter Attacken zusammen und können abgeglichen werden.

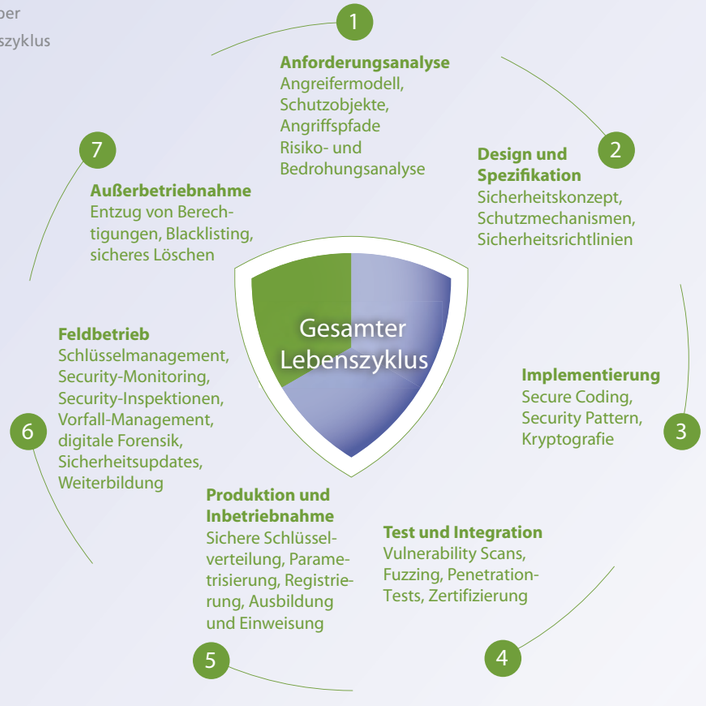
Gesamtflotte als Basis für dynamische Schutzstrategie

Aus der Analyse der Daten bekommen OEMs einen umfassenden, jederzeit aktuellen Überblick darüber, welche Strategien Hacker verfolgen, welche Angriffspunkte sie anvisieren und ob sich Attacken häufen. Zur Auswertung dieser umfassenden Eventdatenbasis in einem Backend greift die nächste Stufe des dynamischen Abwehrsystems: Die automatisierte, auf Big-Data-Methoden basierende Softwarelösung Cycur-GUARD. Diese analysiert die Angriffsmuster und nimmt eine Vorsortierung vor, anhand derer Sicherheitsexperten und Security-Forensiker in einem Cyber Defense Center entscheiden, ob und welche Gegenmaßnahmen einzuleiten sind. Dazu zählen gezielte Anpassungen der Firewall, Updates des CycurIDS-Regelsets – oder die Beseitigung von Schwachstellen in der Software betroffener Steuergeräte in enger Abstimmung mit deren Herstellern. Die getroffenen Maßnahmen können dann „Over-the-Air“ an alle vernetzten Fahrzeuge der Flotte übermittelt werden – selbstverständlich kryptografisch abgesichert. Zusätzlich sind die Updates durch digitale Signaturen vor unbemerkten Veränderungen geschützt.

Fazit

Weil sämtliche erkannten Anomalien aus allen Fahrzeugen im Feld in der zentralen cloudbasierten Eventdatenbank zusammenlaufen, fallen neue Angriffsmuster schnell auf. Mit jedem Fahrzeug, das diesem Verbund angeschlossen ist, wird IDPS intelligenter und abwehrfähiger. Denn da bisher unsichtbare, gegebenenfalls von Firewalls abgeblockte Angriffe in eine ständige Lageauswertung einfließen, lassen sich Security-Maßnahmen schneller und gezielter an aktuelle Risiken anpassen. Im Verbund entsteht so ein Immunsystem für das vernetzte Fahrzeug, dessen Abwehrkräfte durch jeden Angriffsversuch gestärkt werden. Die stetig wachsende Datenbasis und sofortige Weitergabe der Abwehrstrategien an alle Fahrzeuge im Bestand gewährleisten immer umfassenderen Schutz.

Holistischer Schutz über den gesamten Lebenszyklus hinweg.



In fünf Schritten zur „immunisierten“ Flotte.