Schadsoftware an Bord

Cybersecurity ist aktuell eines der Topthemen in der Automobilbranche. Ohne umfassende Sicherheitskonzepte kommen Innovationen bei Connectivity und teilautonomem Fahren nicht mehr ins Auto.

Fotos: Volkswagen, Flaticon, Shutterstock/Vector by

Immer wieder werden Sicherheitslücken publik, bei denen sich Hacker Zugriff auf den Bordcomputer und sicherheitskritische Steuereinheiten verschaffen konnten. Zum Beispiel, indem sie eine Schwachstelle im Infotainmentsystem genutzt haben, um sich auf andere Steuergeräte vorzutasten. Experten sind sich einig, dass die Hersteller schon viel gegen solche Vorfälle unternehmen – doch eine verbindliche Sicherheit für alle OEMs weltweit lässt weiter auf sich warten. „Security wird zum Teil noch einfach wie ein weiteres Tech-Feature behandelt – das funktioniert aber für autonome Autos nicht. Es ist sicherlich das komplexeste Feature in der Fahrzeuggeschichte, bei der die gesamte technische Kette von der Hardware über Steuergeräte, die Kommunikation im und außerhalb des Fahrzeugs bis ins Backend mit einbezogen werden muss“, erklärt Cybersecurity-Berater Marko Wolf von der Bosch-Tochter Escrypt. Zudem müssten Hersteller dazu in der Lage sein, auch 15 oder mehr Jahre später die Software in ihren Autos zu reparieren. Heißt konkret: Infrastruktur und Experten vorhalten, um Patches ausliefern zu können. „Es gibt eine Reihe ganz beachtlicher Initiativen. Dennoch gelingt Cybersecurity im Fahrzeug nur partiell“, bestätigt Kai Grunwitz von NTT Security. Das liege am Unterschied zwischen der Fahrzeugsicherheit, bei der es eine gewachsene funktionale Absicherung gibt, und der relativ neuen Informationssicherheit für Connected Cars.

Viele Schutzmaßnahmen betrachten den Zu- und Abfluss von Daten, nicht aber das, was im Fahrzeug selbst passiert. Passagiere stellen mit ihren unterschiedlichen Endgeräten und deren Übergängen zum Beispiel ins Infotainmentsystem ebenfalls Sicherheitslücken dar. Weil keine Vorgaben an die Endgeräte möglich sind, sei eine extrem adaptive Sicherheitsarchitektur erforderlich, sagt Securityspezialist Grunwitz. „Der Fokus geht klar weg von den Backend-IT-Systemen hin zu dem, was onboard passiert. Es wird zunehmend versucht, anhand von geschotteten Sicherheitsebenen die Sicherheit zu verbessern, ähnlich wie beispielsweise im Flugzeug.“ Zwar gebe es ein solches „Zoning“ bereits, aber nicht aus Securitysicht, sondern eher funktional zum Beispiel nach Bremse oder Infotainment. Nötig seien Risikoklassen mit klarer Trennung und eindeutigen Übergabepunkten, damit ein Cyberangriff oder eine Manipulation nicht auf alle kritischen Fahrzeugbereiche übergreifen kann. Hier werde viel von den OEMs in die Überarbeitung der Architektur investiert. Doch das ist leichter gesagt als getan. „Jedes Thema, das man in der Security anfasst, beeinflusst das gesamte Fahrzeug und unter anderem auch den Benzinverbrauch. Alle Maßnahmen müssen ausbalanciert werden, damit sie nicht WLTP-Compliance-Anforderungen tangieren“, nennt Securityexperte Kai Grunwitz eine weitere große Herausforderung.

Hundertprozentige Sicherheit kann es mit Blick auf Cybersecurity wohl ohnehin nicht geben. „Wichtig ist, bereits auf konzeptioneller Ebene das Risiko so stark zu minimieren, dass ein erster Angriff nicht weiter übergreifen kann“, erklärt Christoph Krauß von der Hochschule Darmstadt und Abteilungsleiter am Fraunhofer-Institut für sichere Informationstechnologie (SIT). Die Erhöhung der Verkehrssicherheit durch vernetztes Fahren werde jedoch wesentlich bedeutsamer sein als die Schäden einzelner erfolgreicher Angriffe, ist sich der Experte für Cyber-Physical Systems und Automotive Security sicher. Das Thema Testing wird die Securityexperten auch weiter intensiv beschäftigen, denn ohne aufwendige individuelle Tests wird es nicht gehen. „Mit standardisierten Tests lassen sich nicht alle IT-basierten Sicherheitsrisiken identifizieren und ausschließen“, sagt Krauß.

> »Mit standardisierten Tests lassen sich nicht alle IT-basierten Sicherheitsrisiken identifizieren und ausschließen«
> Christoph Krauß, Hochschule Darmstadt und Fraunhofer SIT

Als wichtigen Trend sieht man bei NTT das Thema VSOC (Vehicle Security Operations Center), mit dem die IT-Sicherheit von Fahrzeugen dauerhaft überprüft werden kann. Der Dienstleister bietet OEMs die Security-Analyse der massiven Datenmengen an, die im vernetzten Fahrzeug anfallen. Rund 26 Gigabyte sind das ohne Vorverarbeitung pro Fahrzeug und Stunde. Um frühzeitig mögliche Angriffe ableiten zu können,

Good to know

Einfallstor Ladesäule

Speziell mit Blick auf die Elektromobilität sind neue Angriffsvektoren entstanden, zum Beispiel rund um den Ladevorgang. „Wenn Fahrzeuge mit Plug-and-Charge-Standards über das Ladekabel mit der Ladesäule und den daran angebundenen Backendsystemen kommunizieren, lässt sich dieser Weg potenziell ausnutzen“, berichtet Christoph Krauß vom Fraunhofer-Institut für sichere Informationstechnologie (SIT). Die ISO-Norm 15 118 spezifiziert die Kommunikation zwischen Auto und Ladesäule über eine Powerline-Verbindung und ermöglicht die direkte Authentifizierung und Autorisierung des Fahrzeugs. Die Nutzung einer RFID-Karte an der Ladesäule ist nicht mehr notwendig. Über diese Verbindung können perspektivisch auch Updates und andere Dienste realisiert werden. „Potenziell können Ladesäulen manipuliert werden, um darüber Angriffe durchzuführen“, meint Krauß. „So könnte ein Angreifer auf Kosten eines Dritten laden oder er könnte versuchen, das Lastmanagement anzugreifen, um das Stromnetz zu beeinflussen.“

nutzt das Unternehmen ein auf Machine Learning basiertes IT-Verfahren, das in den Automotive-Bereich überführt wurde. Es hilft, die immensen Datenmengen zu korrelieren und zu analysieren, bevor sie erfahrene Cybersecurity-Analysten im VSOC final bewerten. Auch Marko Wolf meint, dass die Analyse von Mustern entscheidend sei, um Angriffe frühzeitig zu erkennen. Zudem hätten viele Unternehmen mittlerweile dedizierte Response-Teams, die Entwicklungen sowohl im Internet als auch im Darknet beobachten. Sie besuchen auch Hackerkonferenzen, um frühzeitig zu erkennen, ob eine neue Sicherheitsgefahr bestehe. Das Security Incident and Emergency Management werde immer entscheidender. „Man muss dann die Leute, Abläufe und Durchgriffsmöglichkeiten haben, um entsprechend schnell zu reagieren, und Experten an Bord holen, um die Situation zu bewerten und Patches in kurzer Zeit vielleicht an Millionen Fahrzeuge zu verteilen“, so Wolf.

Die Technischen Überwachungsvereine treibt das Thema Cybersecurity auch um. „Noch gibt es keinen Security-TÜV für Fahrzeuge, aber hier wird überlegt, wie man IT-Sicherheit zertifizieren kann“, meint Christoph Krauß. Durch immer neue Bedrohungen sei eine Überprüfung alle zwei Jahre unzureichend, der Betrieb eines VSOC ein alternativer Ansatz: „Ob jeder Hersteller ein eigenes VSOC für seine Flotte betreibt oder dies Organisationen wie der TÜV übernehmen, ist noch unklar. Aber das Thema wird kommen, weil die Live-Überwachung eine sehr wichtige Komponente bei vernetzten und autonomen Fahrzeugen ist“, so Krauß. Das Risiko ist vor allem dort hochkomplex, wo es um Car-to-X-Kommunikation und die datenschutzgerechte Abbildung mehrfach verschachtelter Zertifikate geht. Hier haben selbst kleine Fehler umfangreiche Auswirkungen. Vor Kurzem ging zum Beispiel ein Firefox-Problem durch die Medien: Alle Plug-ins müssen signiert sein, aber das Unternehmen hatte nicht darauf geachtet, dass das zugehörige Prüfzertifikat abgelaufen war – bei Milliarden Nutzern funktionierten plötzlich die Plug-ins nicht mehr. Im Fahrzeug könnten die Risiken in solchen Fällen ungleich gravierender sein. Auch beim Thema Update over the Air ist noch nicht das letzte Wort gesprochen. Besonders stark beschäftigt die Automotive-Unternehmen das Thema Softwaresignaturen. Wenn Updates im Fahrzeug erfolgen, müsse die genaue Verifikation der Softwarestände noch mehr optimiert werden – nicht zuletzt, weil es immer mehr eigenentwickelte Software zum Beispiel für autonome Fahrzeuge bei Autosar gebe, sagt Kai Grunwitz: „Codesignaturen sind nötig, damit nur Softwarepakete installiert werden, die eine Securityfreigabe haben.“ Nur so lasse sich verhindern, dass böswillig beim Hersteller gefährliche Software ins Auto eingebracht wird. Dafür ist DevSecOps, also eine integrierte Security im kompletten Entwicklungsprozess, erforderlich. So lässt sich absichern, welche Softwarebausteine in welchem Modul von wem entwickelt und getestet wurden. „Die Security nachträglich hineinzuprüfen, ist beliebig schwierig und oft nicht möglich“, konstatiert Grunwitz.

Autorin: Daniela Hoffmann