„Security für das Auto: von Grund auf neu zu denken?”

Autos gehen online – ist die Automobilindustrie auf die damit verbundenen Sicherheitsrisiken vorbereitet? Ein Expertengespräch mit Giesecke+Devrient, Consulting4Drive und IAV

Das „Connected Car“ bietet viele geschäftliche Chancen – etwa nachrüstbare Funktionen, datenbasierende Services und immer umfangreichere Fahrassistenzsysteme. Mit der Kommunikationsfähigkeit und Flexibilität kommen aber auch Risiken und Gefahren ins Auto. Gegen derartige Bedrohungen hat die kommerzielle IT eine Reihe von Maßnahmen und Verfahren entwickelt – aber lassen die sich so ohne Weiteres auf das Auto übertragen? Im Expertengespräch diskutieren Dr. Christian Schläger, Leiter Produktmanagement Cyber Security beim Spezialisten für mobile Sicherheitstechnologien Giesecke+Devrient, Timm Kellermann, Geschäftsführer der IAV-Managementberatung Consulting4Drive sowie Kai Feuerstake, Fachbereichsleiter Hard- und Software, Security bei IAV, über die erforderlichen Änderungen in der automobilen Wertschöpfungskette und in den Entwicklungsprozessen. Das Gespräch moderierte Christoph Hammerschmidt, Fachjournalist mit Schwerpunkt Fahrzeugelektronik und -IT.

Autos werden zunehmend autonom, gehen online, sind connected, sie werden zu Teilnehmern an Datendiensten. Damit setzen sie sich auch den Risiken aus, die im Cyberspace lauern. Wie gut ist die Autoindustrie auf die Herausforderung vorbereitet, die daraus resultiert?

Feuerstake: Security ist in der Automobilindustrie kein neues Thema, denn es ging schon immer um den Schutz des Autos und dessen Komponenten – denken Sie an die digitalen Schlüssel und Zugangsmechanismen oder auch die Wegfahrsperre. Bei der Anbindung von Datendiensten und der Cloud werden zudem gängige Security-Techniken eingesetzt wie etwa Authentifizierung und Verschlüsselung. Was definitiv noch fehlt, sind entsprechende Security-Mechanismen zwischen den Steuergeräten und Komponenten im Fahrzeug. Die notwendigen Verfahren erfordern nicht unerhebliche Rechenleistung und belasten den Netzwerkverkehr immens. Die Diskussionen gehen daher – neben Überlegungen zur notwendigen Standardisierung wie zum Beispiel bei Adaptive AUTOSAR – stark in Richtung Fahrzeug-/Sicherheitsarchitektur und um die Frage, wie viel Security man sich leisten kann bzw. will.

Kellermann: Ich denke, dass die Größenordnung dessen, was wir künftig unter Security verstehen müssen, sich massiv ausweitet. Das Thema wird viel umfangreicher, und auch die Konsequenzen eines möglichen Cyberproblems werden viel gravierender sein als bisher. Was würde beispielsweise passieren, wenn ein autonom fahrendes Auto per Cyberangriff zu einer Waffe würde? Die Verantwortung, dieses Risiko abzusichern, ist in den letzten Jahren deutlich größer geworden.

Schläger: Im Auto findet sich die Frage der Sicherheit in konzentrierter Form: Es geht um Kundendaten, um Mehrwertdienste, die auf Personen- und Bezahldaten zugreifen. Dieses Thema ist aus der Industrie bekannt, wo man mit der Absicherung von Maschinen schon eine gewisse Erfahrung hat. Beim Auto kommt aber die Mobilität hinzu. Das macht die Frage der Sicherheit – Safety und Security, die voneinander abhängen – sehr komplex. Andererseits besitzen die OEMs bereits Mechanismen, um solche Dinge zu kontrollieren. Sie haben ihre Security-Operating-Center, sie haben ihre Incident- und Event-Prozesse. Das müssen sie jetzt auf den „Endpunkt Fahrzeug“ mit all diesen Ebenen ausdehnen. Wir wissen ja, wie viele Fahrzeuge alleine wir von G+D Mobile Security mit unseren SIM-Karten online bringen. Das Auto ist bereits ein IoT-Element, und zwar in relativ großen Zahlen. OEMs machen sich also nicht erst heute Gedanken darüber, wie sie das managen wollen.

In Zukunft wird auch die Software in den Fahrzeugen online aktualisiert werden. Bringt das nicht eine ganz neue Dimension in die Autos?

Schläger: Ja, aber andererseits ist das die einzige Chance, ein Auto über seinen Lebenszyklus hinweg sicher zu halten. Das Hauptproblem, das wir sehen, ist der lange Lebenszyklus der Fahrzeuge. Bei den Sicherheitschips, die wir heute in eine Master- oder Visakarte einbauen, haben wir eine Lebensdauer von drei Jahren, danach ist die Karte ungültig. Bei einem Fahrzeug haben wir Lebenszyklen von zehn, fünfzehn Jahren oder noch länger. Da kann natürlich auch immer wieder mal etwas aktualisiert werden, aber nicht die Hardware. Das muss ich mit Software-Updates over the air machen. Wichtig ist die Frage der Taktung solcher Security-Updates. Im IT-Umfeld sind wir mittlerweile bei einem maximal monatlichen Rhythmus angelangt. Aber bei einem Auto – welche Serviceintervalle hat man da heute? Zwei Jahre? 15.000 Kilometer? Zwölf Monate? Das ist für die Aktualisierung von Software viel zu lang. Da kann man nur dann Erfolg haben, wenn man die Software auch schnell bei Bedarf über Online-Mechanismen

aktualisiert, über einen sicheren Kanal. Sonst hat man keine Chance.

Kellermann: Genau! Die Häufigkeit, aber auch der Umfang dieser Updates stellen eine völlig neue Dimension dar. Wir in der Autoindustrie sind gerade in eine interessante Zwickmühle geraten: Wir glauben, dass wir sehr viel Wert schöpfen können, indem wir Fahrerassistenzsysteme in die Autos einbauen. Das entlastet den Fahrer, es senkt den Stresslevel. Gleichzeitig bedeutet es, dass wir fahrkritische Software auch im Feld kontinuierlich verbessern müssen. Diese Updates werden im ungünstigsten Fall täglich durchgeführt werden müssen, im Normalfall wohl wöchentlich, vielleicht monatlich. In jedem Fall ist das ist eine Frequenz, die wir in der Automobilindustrie noch nie hatten. Aufgrund dieser Perspektive gehen wir davon aus, dass es im Lebenszyklus eines Fahrzeuges möglich sein muss, einen kleinen Anteil der Elektrik/Elektronik tauschen zu können, um die Sicherheit des Fahrzeugs, der Insassen und der Passanten über den gesamten Einsatzzeitraum ausreichend zu schützen.

Feuerstake: Das wirft noch ganz andere Probleme auf. Heute wird ein Auto nach Markteinführung aus der Entwicklung herausgenommen und an das Aftersales übergeben. An der Steuergerätesoftware wird – Stand heute – nur noch etwas geändert, wenn im Feld gehäuft relevante Probleme auftreten. Die Lieferanten werden dann einzeln für die notwendigen, meist funktionalen Änderungen beauftragt. In Zukunft wird die Forderung dahin gehen, dass die Steuergeräte mit regelmäßigen Sicherheits-Patches versehen werden – und das bis zu 15 Jahre nach SOP. Für diese Anforderung müssen die Entwicklungs-, Freigabe- und Contentmanagement-Prozesse der Hersteller entsprechend angepasst werden. Hier geht es um wahrscheinlich riesige Entwicklungsumfänge, die die Pflege der Bestandssoftware im Feld betreffen. Verschärft wird diese Herausforderung durch die Variantenvielfalt und die notwendigen Absicherungs- und Freigabeverfahren.

Dazu kommt der Umstand, dass per Software komplett neue Geschäftsmodelle ermöglicht werden: zum Beispiel, dass Kunden bestimmte Features des Autos auch nach dem Kauf noch per Software-Update erwerben können.

Timm Kellermann, Geschäftsführer der IAV-Managementberatung Consulting4Drive

Kellermann: Dieser Punkt enthält ebenfalls relevante Aspekte für die Sicherheitstechnik. Denn er berührt das Fahrerprofil aus Benutzerrechten und nutzerspezifischen Funktionen. Wir stellen fest, dass es bei den modernsten Autos immer noch ein sehr schwieriger Vorgang ist, ein Benutzerprofil zu wechseln. Die Autobranche ist bisher nicht besonders gut auf das Identity-Management vorbereitet: Welcher Mensch darf gerade dieses Fahrzeug benutzen – ob privat oder in einem Shared-Mobility-Kontext? Das Auto muss also wissen, wer gerade fährt und welche Rechte er besitzt. Die Lizenzen gelten nicht für das Auto, sondern für den Fahrer. Das ist eine große Umdenkleistung. Es ist ein sehr aufwendiger Prozess, diese Profile zu schützen, gegen Missbrauch abzusichern und eine Nachweiskette über alle Änderungen und die daran beteiligten Personen zu führen.

Schläger: Identitätsmanagement ist tatsächlich eine der Kernfunktionen, die wir im Auto haben werden. Das Auto hat eine Identität, die Steuergeräte haben eine, der Hersteller ebenso und natürlich auch die Fahrer bzw. Flottenmanager. Dies ist im Grunde dem sehr ähnlich, was wir unseren Kunden aus dem Banken- oder dem Telco-Umfeld anbieten. Genau das hat bei vielen unserer Kunden ein Umdenken bewirkt, sodass sie sich jetzt nicht mehr als Produkthersteller, sondern als Serviceunternehmen verstehen. Im Automobilumfeld werden wir das genauso sehen. Diese Identitäten hinsichtlich der Fahrzeugnutzung kann man abspeichern, wo es sicher ist – zum Beispiel im sicheren Bereich eines Mobiltelefons, das ja auch schon als Schlüssel genutzt wird. Ebenso wie dieses sichere Gerät den Zugang zum Fahrzeug gewährt, kann es auch den Zugang zu einem anderen Service verwalten. Das kann auch ein Bezahlservice sein. Es kommt darauf an, dass man in der Lage ist, solche Identitäten sicher verwalten zu können. Wenn man das kann, ist es letztlich egal, welche Technik sich dahinter verbirgt.

Wird also jeder Hersteller eine eigene Plattform zum Identitätsmanagement haben- oder wird es hier einen IT-Standard geben, der für alle Hersteller gilt?

Kellermann: Diese Frage haben wir mehrfach diskutiert und bisher darauf keine finale Antwort gefunden. Wenn man eine technisch ausgereifte Landschaft voraussetzt, wäre es tatsächlich sinnvoll, einen Standard in der Industrie zu haben. Wenn aber eine neue Technologie gerade erst entsteht und unklar ist, welche Lösung erfolgreich sein wird, sind die Voraussetzungen für eine Standardisierung nicht gegeben. Deswegen gehen wir davon aus, dass die OEMs auf absehbare Zeit versuchen werden, ihre eigenen Standards und Plattformen zu etablieren und sich damit einen Wettbewerbsvorteil zu verschaffen. Ob man sich dann auf gemeinsame Schnittstellen, auf Teilstandards oder erweiterte Standards zum Schutz der Gesellschaft und zur besseren Zusammenarbeit mit Geschäftspartnern einigen wird, wird die Zeit zeigen. In diesen letzten beiden Punkten sehe ich ein bedeutendes Potenzial für Standardisierung zu einem frühen Reifegrad.

Feuerstake: Hier stellt sich die Frage, ob es sinnvoll ist, dass sich eine solche Funktion als Standard entwickelt? Diversität hat den Charme, dass nicht gleich alle Einfallstore offen stehen, falls etwas gehackt werden würde.

Muss die Autoindustrie diese Dinge eigentlich selber erfinden? In der IT-Wirtschaft gibt es solche Techniken doch schon seit Jahren; die Banken könnten gar nicht ohne leben. Kann sich die Autowirtschaft bei der Implementierung sicherer Funktionen nicht einfach aus dem Werkzeugkasten der IT bedienen? Oder liegt die Sache bei Autos derart anders, dass man hier eigene Wege gehen muss?

Feuerstake: Man muss nicht alles neu erfinden, das ist auch nicht das Bestreben. Der wichtigste Grund, warum manche Techniken aus der IT nicht direkt auf das Auto übertragbar sind, sind die knappen Ressourcen in den Fahrzeugen. PCs, Server, die Cloud – alle haben im Vergleich zu Fahrzeugsteuergeräten die vielfache Rechenpower. Derart hochperformante Systeme werden wir im Auto in näherer Zukunft so wohl nur in Domainrechnern sehen. Größe, Gewicht und Dauerhaltbarkeit sind die hauptsächlichen Hinderungsgründe, neben dem Kostenfaktor. Ansonsten könnten viele Dinge aus der IT sofort übernommen werden. Natürlich gibt es auch Ansätze und Diskussionen über die Verlagerung von Algorithmen und Funktionen aus dem Auto in die Cloud. Jedoch kann ich mir dies beim Thema Security nur bedingt vorstellen.

Dr. Christian Schläger, Leiter Produktmanagement Cyber Security bei Giesecke+Devrient Mobile Security

Schläger: Es kommt noch ein weiteres Problem hinzu: Es ist nötig, dass jemand das Thema Security zwischen IT und Autowirtschaft „übersetzt“. Da wir aus verschiedenen Industrien kommen, haben wir unterschiedliche Entwicklungszyklen, Vorlaufzeiten und andere Vorgaben und Standards. Das unterscheidet die Autoindustrie von klassischer Produktion, Netzbetreibern oder der Bankenindustrie. Es gibt immer wieder unterschiedliche Vorstellungen sowohl bei der Frage, wie wir entwickeln, als auch bei der Frage, wie wir zusammenarbeiten. Andererseits sehe ich auch, dass die IT gerade in der Frage der Zuverlässigkeit vieles von der Autoindustrie lernen kann. Und der Begriff „langfristig“ hat in der IT eine ganz andere Bedeutung als bei Ihnen.

Kellermann: Ich denke, es lohnt sich, hier genauer hinzusehen. Ein Lebenszyklus von zehn, fünfzehn Jahren ist eine sehr lange Zeit bei IT- und Sicherheitsfragen. Das heißt, wir müssen uns intensiv Gedanken machen, wie viel Flexibilität wir ins Auto hineinbringen wollen bezüglich Hardwaretausch und Softwarepflege-Zeiträumen. Das Zeitalter der digitalen Plattformökonomie ist gerade erst angebrochen. Aber eine Erkenntnis zeichnet sich jetzt bereits ab: Flexibilität der Fahrzeug- und Backendsysteme liefert im Internet der Dinge sowohl unter Sicherheitsgesichtspunkten als auch unter Kundenorientierungsaspekten einen deutlich höheren faktischen Mehrwert, als dies in der Automobilindustrie bisher der Fall war.

Zudem haben sich die Randbedingungen verschoben. Auch in der Vergangenheit waren Autos online, aber das waren sie eher unterstützend oder ausnahmsweise. In der Zukunft ist

das Auto als Device im Internet of Things (IoT) grundsätzlich online und wird auch so gemanagt. Der Offline-Zustand kommt vor und es gibt Sonderprozesse hierfür. Bei einem Auto kommt, im Gegensatz zu einer Bank, der Aspekt der Physik hinzu. Ein Auto fährt und stellt damit eine physische Gefahrenquelle dar. Menschen, die im Auto sitzen, müssen geschützt werden, ebenso die Menschen in ihrer Umgebung. Das zeigt, dass die Begriffe Security und Safety nicht vollständig voneinander entkoppelt werden können. Wir müssen daher nicht nur die technische Architektur reflektieren, sondern auch die Abläufe oder Prozesse, die den Nutzer in seinem Mobilitätskontext schützen. Bisher wurden Autos gebaut und aus dem Fabriktor gerollt. Herr Schläger hat aufgezeigt, dass wir künftig wahrscheinlich im Abstand von wenigen Wochen ein Update fahren müssen, vielleicht sogar öfter.

Schläger: Ich neige dazu, zu widersprechen. Wir haben im Maschinen- und Anlagenbau ähnlich lange Produktlebenszyklen. Wir haben es heute mit Maschinen zu tun, die sind noch aktiv im Feld, während andere Exemplare aus der gleichen Serie bereits im Deutschen Museum stehen.

Feuerstake: Aber nicht in den Stückzahlen wie im Automobilbau. Und sind diese Maschinen ans Netz angebunden?

Schläger: Doch, die sind mittlerweile angebunden. Wir haben dafür eine Lösung: Produkt und Security trennen. Die Maschine bekomme ich nicht mehr upgedatet, aber wir schalten eine Security-Komponente auf einer Extra-Hardware davor, die eine Gatekeeper-Funktion wahrnimmt. Damit gibt es eine Grenze, die sich kontrollieren lässt. Bei einem System wie dem Auto, das ich aus der Hand gebe, ist das natürlich etwas anderes als bei einer Maschine.

Feuerstake: Genau das ist der Knackpunkt. Ein potenzieller Angreifer, der Fahrzeuge hacken und später von der Ferne aus darauf zugreifen will, wird sich zunächst ein oder mehrere Exemplare kaufen und sich damit intensiv beschäftigen. Das werden wir nicht verhindern können. Dieses Risiko ist im Maschinen- und Anlagenbau so nicht unbedingt gegeben.

Schläger: Das ist richtig. Aber da kann man von den Herstellern mobiler Geräte lernen, die dasselbe Problem haben: Die werfen von einem Gerät eine Million Stück oder mehr auf den Markt und wissen, jeder wird es erst einmal in die Hand nehmen und versuchen, die Sicherheitsfeatures zu brechen. Dafür greifen diese Hersteller auf die traditionellen Ansätze aus der IT zurück: Man muss die Geräte ebenso wie den Kontext ihres Gebrauchs monitoren, man muss einen Detection-Mechanismus für Fraud haben und man braucht Prozesse, um sehr schnell reagieren zu können. Aber um eine solche Flotte an Fahrzeugen und Geräten zu managen, sind eine ganz andere Infrastruktur und eine Architektur an Prozessen, an Kapazitäten etc. erforderlich.

Kellermann: Diese Security-Analytics-Komponente – also Fraud-Detection, Monitoring etc. – ist im künftigen Automobilitätsrahmen wirklich sehr groß und wichtig geworden. Ich sehe kaum eine Parallele zu einer Anwendung in einer anderen Branche, die eine solche Brisanz hat – sowohl was die Stückzahlen anbelangt als auch die Relevanz für die Gesellschaft. An dieser Stelle betreten wir als Industrie Neuland, weil wir die Technologien, Prozesse und Antwortmechanismen für die Automobilindustrie neu kombinieren müssen. Das wird schon allein an einer Dimension offensichtlich: Wenn ich erkenne, dass in der von mir überwachten Flotte eine sicherheitsrelevante Irregularität auftaucht, muss ich in der Lage sein, unter Umständen innerhalb von Minuten zu reagieren und ein Notfallprogramm zu aktivieren. Diese Fähigkeiten haben wir so in der Vergangenheit nicht gehabt. Für militärische Anwendungen und für andere Anwendungsbereichen mit geringen Stückzahlen gibt es das durchaus. Aber die Kombination aus massenhafter Verbreitung, Mobilität, inhärentem Gefahrenpotenzial aufgrund der Geschwindigkeit, und dann noch hochkomplexen, in Zukunft wesentlich auf Software basierenden Funktionen, das ergibt eine ganz neue Dimension. Hier ist es nötig, über unterschiedliche Kompetenzfelder hinweg neue Lösungen für die Autoindustrie zu entwickeln.

In der IT-Security-Branche hat man dafür CERTs (Computer Emergency Response Teams). Das sind Teams, die auf solche Probleme reagieren können. Wäre das ein gangbarer Weg?

Kai Feuerstake, Fachbereichsleiter Hard- und Software, Security bei IAV

Schläger: Solche CERT-Systeme kennen wir nur aus geschlossenen Systemen, etwa bei Betreibern kritischer Infrastrukturen. Die müssen auch in Echtzeit reagieren. Aber dabei handelt es sich wieder um ortsfeste, kontrollierte Anlagen. So ein CERT-Modell kann ich nicht einer Flotte von Fahrzeugen überstülpen. Letztlich müssen Sie Einzelfallentscheidungen treffen: Was läuft in diesem konkreten Auto, an dieser Stelle und mit diesen Insassen gerade richtig oder falsch?

Feuerstake: Das Thema müssen die OEMs zwangsläufig auf ihre Agenda setzen. Der Kunde wird erwarten, dass die zweitgrößte Lebensinvestition nach dem Hauskauf gut gesichert und vor Manipulation geschützt ist. Es wird in der Regel nicht reichen, einen Angriff zu detektieren und abzuwehren – es wird darauf ankommen, die Ziele des Angreifers herauszufinden. Für den OEM oder einen Flottenbetreiber ist diese Information natürlich hoch spannend. Denn damit kann er seine Abwehrstrategien verbessern und gegebenenfalls prädiktive Aussagen über zukünftige Problemfelder machen. Ein solches Monitoring müsste relativ detailliert ablaufen, eventuell sogar bis auf die Steuergeräteebene. Über die folgenden Schritte hinsichtlich der Schließung von Sicherheitslücken und der notwendigen Einbeziehung der SG-Lieferanten bis zum EOL (End of Life) habe ich ja bereits gesprochen. Jedoch habe ich heute noch keine klare Vorstellung davon, welche Strategien gewählt werden müssen, wenn eine Flotte gehackt oder infiziert wurde und nicht umgehend ein entsprechender Patch zu Verfügung steht. Das Auto einfach nicht mehr zu benutzen – wie man es vielleicht mit dem heimischen PC machen könnte – ist sicherlich kaum eine Option. Das alles sind sehr spannende Fragen und Aufgaben, denen wir uns stellen müssen.

Kellermann: Im Grunde lassen sich diese Sicherungsszenarien in drei Bereiche einteilen. Erstens: Mein Konsument bzw. mein Kunde versucht sich eine Leistung zu erschleichen, die er nicht bezahlt hat. Zweitens: Ich habe es mit einer kriminellen Energie zu tun, die sich auf einen Hersteller oder auf eine Kundengruppe bezieht, oder drittens: Ich habe eine terroristische Energie, die sich gegen die Gesellschaft richtet. Da stecken sehr komplexe Bedrohungs- und Risikoszenarien drin. Sie sind nicht grundsätzlich neu, sondern neu im Kontext der Automobilindustrie. Angesichts dessen sind wir gut beraten, Sicherheit branchenübergreifend grundlegend neu zu denken – als Element von Architektur und Prozess unserer IoT-Produkte und -Services und nicht nur unter dem Technologieaspekt. Das betrifft den Aufbau unserer Prozesslandschaft sowie unserer Zulassungsverfahren und Regularien. „Secure and safe by Design" – wir haben versucht, bei der Entwicklung von Steuergeräten schon so zu denken, desgleichen beim Steuergeräteverbund. Aber in dem Kontext, den wir eben diskutiert haben, mit seinen vielen neuen Nutzungs-, aber auch Missbrauchsszenarien, müssen wir die Architektur der Prozesse und Lieferbeziehungen unter den Aspekten Safety und Security sehr sorgfältig auf Handlungsbedarfe hin reflektieren.

Kontakt:
kai.feuerstake@iav.de
t.kellermann@consulting4drive.com
christian.schlaeger@gi-de.com