© Nico Bohnert

„Security mit mehr Pragmatismus angehen“

Die Automobilbranche nutzt die langjährigen Erfahrungen von IT-Security-Spezialisten anderer Branchen. Im Interview mit Sebastian Labitzke erklärt der Security-Verantwortliche von ITK Engineering, wie das Technologie-Unternehmen diese Kompetenzen mit Automotive Safety und Security in Einklang bringt sowie neue Prozesse und Lösungen erarbeitet.

Sebastian Labitzke (Jahrgang 1982) arbeitet seit 2014 bei der ITK Engineering AG im Themenkomplex Security. Neben der disziplinarischen Führung zweier Security-Engineering-Teams an den ITK-Standorten Rülzheim (Zentrale) und Berlin, koordiniert er firmenweit die ITK-Security-Projekte. Aufgrund seiner Expertise im Bereich der IT-Sicherheit steuert er ferner das Managementsystem für Informationssicherheit der ITK. Seine fachlichen Schwerpunkte liegen auf Angreifer-Typisierungen, Threat- und Risikoanalysen und dem Protokoll-Design zur Absicherung digitaler Kommunikation.

Labitzke studierte Informatik an der Universität Karlsruhe (TH) und promovierte anschließend am Karlsruher Institut für Technologie (KIT) im Bereich der Telematik mit den Security-nahen Schwerpunkten Identity- und Access-Management sowie Privacy Enhancing Technologies im Umfeld von Enterprise-Anwendungen und Online Social Networks. Als Mitarbeiter des Steinbuch Centre for Computing (SCC) sammelte er rund sechs Jahre Erfahrung in Projekten dieses Rechenzentrums und des Verbunds der Rechenzentren der Universitäten des Landes Baden-Württemberg.

ATZelektronik _Herr Labitzke, ITK Engineering unterstützt schwerpunktmäßig Kunden aus der Automobilindustrie bei der Entwicklung, Integration und Absicherung von Steuergeräten und Software. Für ITK und die Automobilbranche generell ist das Themenfeld Security vergleichsweise jung – somit gilt es, das entsprechende Know-how erst einmal aufzubauen und aus anderen Branchen zu lernen. Wie überzeugen Sie als relativ junger Security-Lösungsanbieter?
LABITZKE _ ITK investiert seit über sechs Jahren in Embedded Security im Automobil. Die Automotive Security ist generell ein junges Aktionsfeld, wenn man sie mit der klassischen IT-Security vergleicht, die seit den 90er-Jahren dringend notwendige Sicherheitslösungen bereitstellen muss. In unserem mittlerweile 35-köpfigen Security-Team arbeiten auch Spezialisten, die über zehn Jahre Erfahrungen in der IT-Security mitbringen und in anderen Branchen an entsprechenden High-Tech-Lösungen mitgearbeitet haben. In allen Disziplinen, die dafür notwendig sind, zum Beispiel IT-Security, Protocol Security (Telematik), Mobile App Security sowie Embedded Security.

Wo liegen Ihrer Meinung nach Alleinstellungsmerkmale von ITK gegenüber Unternehmen mit langgedienten IT-Security-Spezialisten?
Wir kennen das Automobilgeschäft sehr gut, die Prozesse, die Planungen und die Notwendigkeiten unserer Kunden. Seit über 22 Jahren beraten und entwickeln wir im Bereich der Embedded Systems, insbesondere auch in der Safety und der Umsetzung von Sicherheitslösungen. Die Bündelung unserer Erfahrungen aus dem Embedded-Bereich haben wir mit Security-Know-how angereichert. Wir gehen dabei sehr pragmatisch vor. Das heißt beispielsweise, wir beraten nur Dinge, die wir auch wirklich entwickeln- und umsetzen können. Es mögen Vorgehensweisen und durchaus bestätigte Theorien und gut gemeinte Leitfäden für die Umsetzung von Security-Maßnahmen niedergeschrieben sein. Man muss aber genau hinschauen und interpretieren, was sich kundenindividuell und anwendungsbezogen überhaupt realisieren lässt. Manche Unternehmen starten erst einmal mit einer Risikoanalyse, leiten dann einen Maßnahmenplan ab und kommen dann spätestens in das Tal der Tränen. Denn sie sehen sich einer Unmenge von Anforderungen und Risiken gegenüber. Die Enttäuschung kann man verhindern, wenn man frühzeitig diejenigen Security-Entwicklungsingenieure an Analysen und Umsetzung setzt, die aus dem automobilen Embedded-Bereich kommen, Ingenieure, die Restriktionen in Steuergeräten kennen und zudem Security nicht nur beraten, sondern auch umsetzen können. Dann haben wir eine realistische Chance,

„Zielkonflikte zwischen Safety und Security lassen sich lösen“

zu einem Security-Maßnahmenkatalog, einer sicheren Architektur und sicheren Protokollen zu kommen, die letztendlich umsetzbar sind.

Es gilt, die Balance zwischen Safety, Security und Kosten zu finden. Welche Wechselwirkungen, Zielkonflikte und Synergien sehen Sie?
Zunächst einmal ist es wichtig, in der Security das hohe Niveau an Standards und integrierten Prozessen zu erreichen, wie wir sie in der Safety mit der ISO 26262 etabliert haben. Das bedeutet, wir müssen hier investieren. Kosten sind immer und überall ein maßgebendes Kriterium. Unter anderem mit möglichst vielen Synergien zwischen Safety und Security können wir diese entsprechend klein halten. Es ist dabei nicht zielführend, beide Disziplinen in einem gemeinsamen Prozess zu synchronisieren, sondern vielmehr Schnittstellen zu schaffen, und damit eine Kollaboration und gegenseitige Befruchtung zu ermöglichen.

Könnten Sie dies anhand eines Beispiels beschreiben?
Etwas vereinfacht lassen sich Synergien an der elektrischen Parkbremse verdeutlichen. Die Funktion sorgt für Sicherheit, indem sie nach dem Parken oder mit der zusätzlichen Funktion des Berganfahrassistenten ein Wegrollen verhindert sowie ein sicheres Anfahren unterstützt. Neben Safety lässt sich in die Parkbremse auch Security integrieren, nämlich der Diebstahlschutz.

„Manche Unternehmen starten erst einmal mit einer Security-Risikoanalyse, leiten dann einen Maßnahmenplan ab und kommen dann spätestens in das Tal der Tränen“, erläutert Sebastian Labitzke und verweist dabei auf pragmatischere Vorgehensweisen

Und welche Zielkonflikte lassen sich wie lösen?
Anschaulich ist das Beispiel einer Airbagauslösung. Die Anforderung an die Safety-Ingenieure ist hier, den Airbag in einer Gefahrensituation zum exakt richtigen Zeitpunkt und dann so schnell wie möglich, mit möglichst wenig Latenz, auszulösen. Die Security-Ingenieure hingegen müssen sicherstellen, dass es sich bei dem Auslösevorgang nicht um eine Fehlauslösung handelt, etwa durch einen Angriff von außen provoziert. Das tun die Fahrzeugentwickler, indem sie kryptografische Maßnahmen zwischenschalten. Und dieses Zwischenschalten kostet die wertvolle Zeit, die sich Safety-Ingenieure hart erarbeitet haben. Der Konflikt kann nur mit den erläuterten neuen Prozessen gelöst werden …

… die ja noch nicht etabliert sind und heute auf Schwachstellen hinweisen?
Es bedeutet heute noch Aufwand, um zu adäquaten und effizienten Prozessen zu kommen. Diese müssen auch schleunigst verbessert werden. Meiner Ansicht nach sind viele Unternehmen auf einem guten Weg, Security in die frühen Entwicklungsphasen zu integrieren. Ein zugebenermaßen anspruchsvoller Weg, der uns als ITK die Chance gibt, in der Beratung und Begleitung wirklich Großes zu bewegen.

Gibt es einen Fahrplan für anstehende Verbesserungen und Weiterentwicklungen im Security-Sektor?
Die Entwicklung von Standards wird diskutiert und sukzessive in Gremien erarbeitet. Die Grundlagen dieses zu tun, sind da. Doch eine Art Handbuch der Security wird es in naher Zukunft nicht geben und dieses würde auch keinen Sinn machen. Auch wenn wir an Standardarchitekturen arbeiten, letztendlich muss Security individuell entwickelt werden, möglichst modular und auf Basis von State-of-the-Art-Kryptografie.

Sie betonten zuvor das kollaborative und parallele Entwickeln, und nun aber das Individuelle.
Das ist kein Widerspruch. Die Kryptografie an sich muss sich weiterentwickeln. Denn die Welt der Security ist enorm dynamisch. Die Angreifer können heute noch nicht das, was sie sicherlich morgen perfekt beherrschen. Zur Verteidigungsstrategie gehört die Modularität der Security, um beispielsweise Verfahren über eine vorzusehende Update-Fähigkeit schnell austauschen zu können, ohne gleich gesamte Fahrzeugflotten zurückzurufen.


© Nico Bohnert

„Start-ups und potenzielle Start-ups geben fantastische Impulse, die für die Fahrzeugindustrie unfassbar wichtig sind“, erklärt Labitzke

„Neue Teams von Security-Experten werden benötigt“

Immer mehr Experten sprechen eher von einer notwendigen Revolution der Fahrzeugarchitektur und geben evolutionären Entwicklungen weniger Chancen. Wie wägen Sie ab?
Es wird beide Welten geben, je nachdem, wie viele Features in welchem Zeitraum realisiert werden müssen. Die Security-Experten entwickeln Lösungen für beide Ansätze. Auf revolutionären Architekturen lässt sich Security schneller und besser integrieren, ob sich diese im System allerdings schneller realisieren lassen, bleibt meiner Ansicht nach heute noch offen. Auf der grünen Wiese oder in periodisch immer wieder neu designten Systemen lässt sich das ausprobieren. Die evolutionäre Weiterentwicklung wird weiterhin überwiegen. Für die Branche ist es schon revolutionär genug, von komponentenbasierten Architekturen in die funktionsorientierten zu migrieren.

Consumer-Elektronik für das Automobil (CE4A) birgt große Herausforderungen. Welche Spezialthemen sehen Sie?
Wir müssen mit offenen Systemen umgehen und mit den vielschichtigen Herausforderungen der Konnektivität stehen Automotive-Security-Ingenieure vor komplett neuen Aufgaben. Aus dem Consumer-Bereich kommen beispielsweise Apps, die in die Fahrzeugsteuerung eingreifen. Spätestens dann ist die höchste Alarmstufe erreicht. Neue Teams von Security-Experten werden benötigt und zwar aus unterschiedlicher Domänen: der IT-Security und der Automotive Embedded. Es müssen zudem Experten für Protokolle und Architekturen an denselben Tisch, genauso wie die Mobile-App-Entwickler.

Gibt es diesen Tisch?
Bei ITK bringen wir die Vertreter dieser Domänen seit sechs Jahren zusammen. Wir leben diesen Austausch und das bringt uns und die Security-Lösungen enorm gut weiter. Anfangs gab es noch gar keine Kundenaufträge und wir führten über das gemeinsame Engagement in Arbeitskreisen hinaus zunächst interne Projekte durch. Für die Security-Community haben wir beispielsweise Benchmarking von Kryptografie-Algorithmen auf Fahrzeugsteuergeräten betrieben. All das nutzt uns nun in heutigen realen Serienentwicklungen – in erster Linie unter technischen Gesichtspunkten und durchlaufenen Reifeprozessen, aber auch hinsichtlich eines nachhaltig aufgebauten Vertrauensverhältnisses und einer eingespielten Zusammenarbeit.

Viele Jahre hat es gedauert, um die ISO 26262 aufzubauen und zu etablieren. Den Luxus der Zeit hat die Branche bei vergleichbaren Standards für Security nicht. Wie navigieren Sie und Ihre Kunden?
Die Zeit haben wir in der Tat nicht. Und ich möchte nichts schön reden. Doch den derzeitigen Veränderungs- und Findungsprozess finde ich spannend, im positiven Sinne. Parallel zu den laufenden Standardisierungen gilt es die Prozesse aufzubauen. Diejenigen Unternehmen, die sich mit dem Status des längst nicht abgeschlossenen Standardisierungsprozess beschäftigen sowie mit stetigen Anpassungen und Nachrüstungen in ihren Organisationen und Produkten auf der Höhe der Zeit bleiben, erarbeiten sich derzeit einen Wettbewerbsvorteil. Und sie sparen sich die hohen Kosten einer späteren Anpassung.

Nicht nur die technischen und prozessualen Veränderungen vollziehen sich enorm dynamisch, sondern auch das Rennen um die besten Akteure, mögliche Kooperationen oder Zukäufe. Wie bewerten Sie in diesem Zusammenhang die Start-up-Szene?
Es ist spannend zu beobachten, wie Start-up-Unternehmen im Markt agieren, wie man versucht, sie zu integrieren und welche Relevanz sie dabei bekommen. ITK erlebt und führt den Austausch hautnah und wir erarbeiten uns Perspektiven. Start-ups und potenzielle Start-ups geben fantastische Impulse, die für die Fahrzeugindustrie unfassbar wichtig sind.

Sehr geehrter Herr Labitzke, ich bedanke mich für das aufschlussreiche Gespräch.

INTERVIEW: Markus Schöttle