Cybersecurity für das Software-definierte Fahrzeug

Unterwegs in die Gefahrenzone

(Bild: depositphotos/Adikk, ETAS)

Das Software-definierte Fahrzeug markiert die nächste Evolutionsstufe der Mobilität: Den Autofahrern verheißt es ein individuelles, sich stetig verbesserndes Fahrererlebnis, den OEMs verspricht es neue Marktchancen jenseits ihres traditionellen Geschäfts. Wirklichkeit werden diese Träume nur, wenn die Fahrzeuge wirksam gegen Cyberangriffe geschützt sind.

Von Carina Böttcher und Dr. Thomas Wollinger

Der Trend scheint klar: In Zukunft wird die Funktionalität und Unterscheidbarkeit von Fahrzeugen nicht länger durch ihre Hardware definiert, sondern durch die darüberliegende Software. Das so lange kolportierte »Smartphone auf Rädern« soll mit dem Software-definierten Fahrzeug (Software-defined Vehicle, SDV) nun endlich Wirklichkeit werden. Eine neue Version des Betriebssystems bringt dann womöglich mehr Veränderung mit sich als neue Hardware-Komponenten. Das Fahrzeug tickt künftig entlang von vergleichsweise kurzen Softwareentwicklungszyklen – in hoher Frequenz bereitgestellte Updates und ein vielfältiges App-Angebot von Mobility-Service-Providern sowie Drittanbietern sorgt für personalisierte, sich stetig erneuernde Fahrzeuge und generiert neue kontinuierliche Umsatzströme. Entsprechend verlangt das SDV nach neuen systemischen Voraussetzungen: Auf Leistungszuwachs ausgelegte Hardware, performante Automotive-Betriebssysteme, stabile Over-the-Air (OTA)-Updatefähigkeit und die

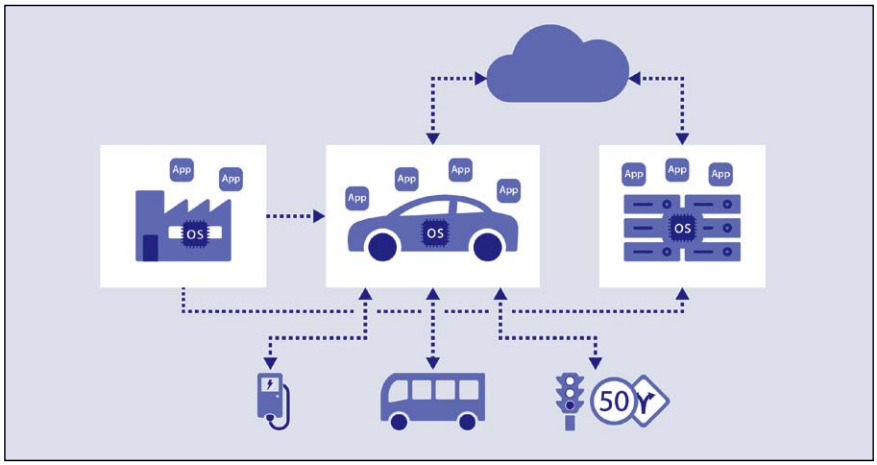

Bild 1. Das Software-definierte Fahrzeug (SDV) ist Teil eines vernetzten SDV-Ökosystem. Softwareanwendungen und Datenaustausch werden vom Betriebssystem des Fahrzeugs verwaltet. (Bild: ETAS)

Berücksichtigung künftiger Anwendungsfälle (V2X-Kommunikation, autonomes Fahren etc.) (**Bild 1**).

Permanente Softwareerneuerung per DevOps-Zyklus

Die Entkopplung von Hard- und Software im Software-definierten Fahrzeug bewirkt eine entscheidende Veränderung: Der Entwicklungszyklus des SDV erstreckt sich damit über die gesamte Lebensspanne des Fahrzeugs. Während in der Vergangenheit jeder Schritt der Entwicklung in sich abgeschlossen war und einer fest definierten Reihenfolge im traditionellen V-Entwicklungsmodell folgend mit Start-of-Production (SOP) endete, wird künftig für das Fahrzeug im Feld ein kontinuierlicher Cloud-basierter Prozess von Softwareentwicklung und -erneuerung entlang des DevOps-Zyklus stattfinden (**Bild 2**).

Diese permanente dynamische »Entwicklungsschleife«, wie sie bei Mobile Devices und PC-Anwendungen längst üblich ist, muss alle Schritte der Fahrzeugentwicklung abdecken und alle am Prozess beteiligten Lieferanten inkludieren. Automotive Cybersecurity darf daher nicht mehr isoliert während der Entwicklung von (Sub-)Systemen betrachtet werden, sondern muss SDV-Lebenszyklus, -Ökosystem und -Zulieferer übergreifend einbeziehen. So muss bereits von Anfang an und immer wiederkehrend in jedem Durchlauf der DevOps-Schleife dafür gesorgt sein, dass nur vertrauenswürdige Komponenten Zugang zum SDV-Ökosystem finden. Ansätze hierfür sind aus der Smartphone-Welt bereits bekannt: Dort ist das Installieren von Third Party Apps nur über einen systemeigenen Marktplatz gestattet. Die angebotene Software muss zwingend definierte Qualitätsstandards und auch Security-Anforderungen erfüllen (sign early and often). Nur dann wird sie vom Systemanbieter in das System eingebunden. Ähnlich könnten in Zukunft auch die OEMs ihr SDV-Ökosystem für vielfältige Software-basierte Leistungsmerkmale, Eigenschaften und Funktionen im Fahrzeug öffnen, ohne dabei die Kontrolle über Qualität, Anbieter und insbesondere auch Security zu verlieren.

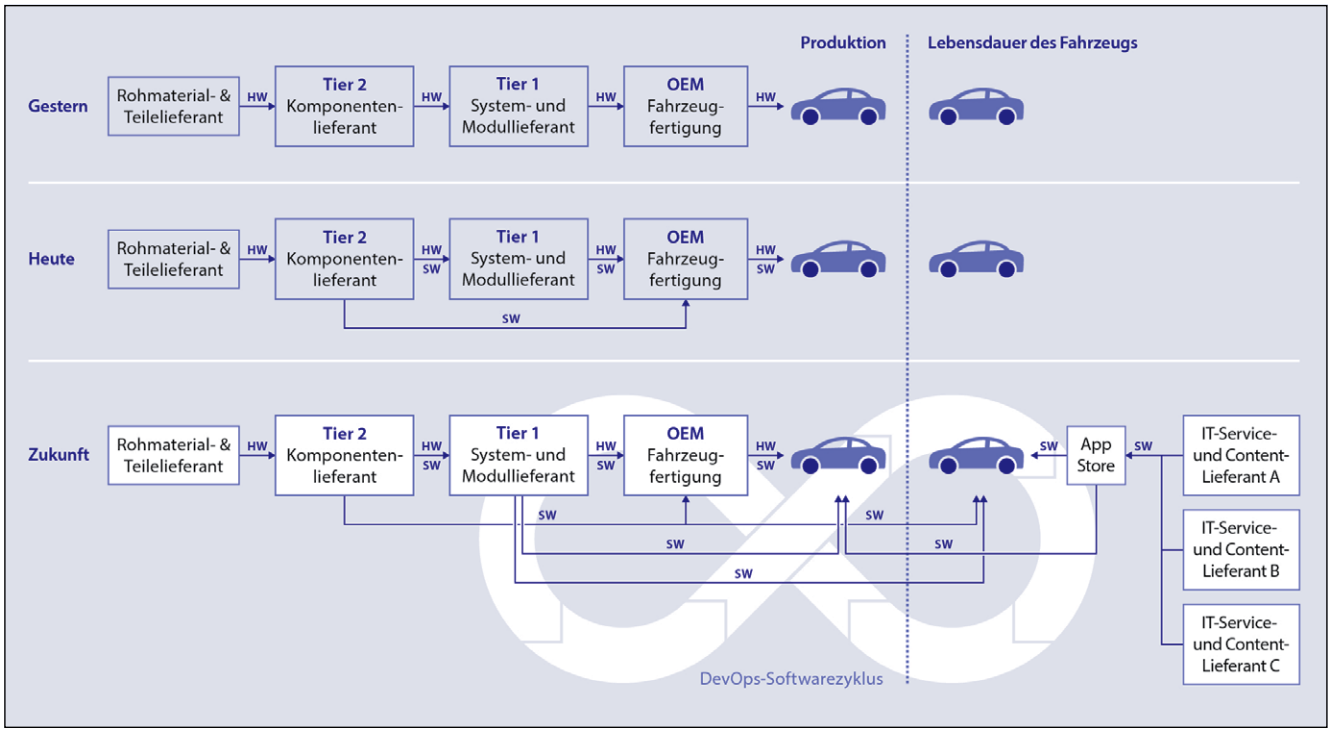

Bild 2. Während in der Vergangenheit die Fahrzeugentwicklung mit Start-of-Production (SOP) endete, wird künftig für das Fahrzeug im Feld ein kontinuierlicher Entwicklungs- und Erneuerungsprozess der Software entlang des DevOps-Zyklus erfolgen. (Bild: ETAS)

Attraktives Angriffsziel

Auf die Cybersicherheit indes hat die Entwicklung hin zum Software-definierten Fahrzeug eklatante Auswirkungen. Die Zahl der möglichen Angriffspunkte nimmt drastisch zu – das betrifft nicht allein die Schnittstellen im Fahrzeug selbst, sondern vor allem auch die potenziell vulnerablen Endpunkte in dessen Ökosystem: Angreifer können sich den unzureichenden Schutz der Fahrzeugproduktion zunutze machen, unerlaubten Zugriff über Cloud-Services erlangen oder auch Schadsoftware mittels Apps von Drittanbietern ins Fahrzeug schleusen. Bei einer derart großen Angriffsfläche und einer ohnehin permanent wachsenden Zahl von Cyberangriffen werden die bisher bekannten, alleinstehenden Security-Mechanismen künftig nicht ausreichen, um das SDV und das zugehörige Ökosystem abzusichern.

Zudem gefährden Cyberattacken dann nicht länger nur die funktionale Sicherheit (Safety) des Fahrzeugs oder der Nutzer- und Fahrzeugdaten (Privacy). Mit dem Wandel hin zum SDV sind künftig auch all jene neuen Geschäftsmodelle und Vermögenswerte bedroht, die die Software-basierte Durchdringung der Fahrzeuge so attraktiv machen. Denn mit dem SDV verlagert sich das Businessmodell der Automobilindustrie hin zu kontinuierlichen Umsatzströmen aus Softwarefunktionen und digitalen Daten – und rückt so ins angestammte Beuteschema für Cyberattacken. Bei unzureichender Absicherung können Angreifer das neue Digitalgeschäft schnell sabotieren, wie sich erst jüngst am Beispiel des Sitzheizungs-Abos eines großen Automobilherstellers zeigte [1].

Doch damit nicht genug: Neue Akteure – etwa die großen Tech-Unternehmen oder auch Drittanbieter von Software und Content – werden künftig das SDV-Ökosystem bevölkern. Zahl und Spektrum zugänglicher Schnittstellen (USB, Bluetooth, WLAN, Mobilfunk etc.) zum Fahrzeug nehmen zu. Außerdem werden die künftigen Software-definierten, automatisierten Fahrzeuge mit ihren 300 bis 500 Mio. Zeilen Softwarecode – drei- bis fünfmal so viele wie ein aktueller Golf 8 – zwangsläufig mehr potenzielle Schwachstellen mitbringen [2]. All das zusammengenommen bildet für Cyberkriminelle einen idealen Nährboden. Bis zur ersten Ransomware-Attacke auf eine Fahrzeugflotte ist es da nur eine Frage der Zeit.

Drei Cybersecurity-Prinzipien für das SDV

Vor diesem Hintergrund ist Automotive Cybersecurity unverzichtbare Voraussetzung für das Software-definierte

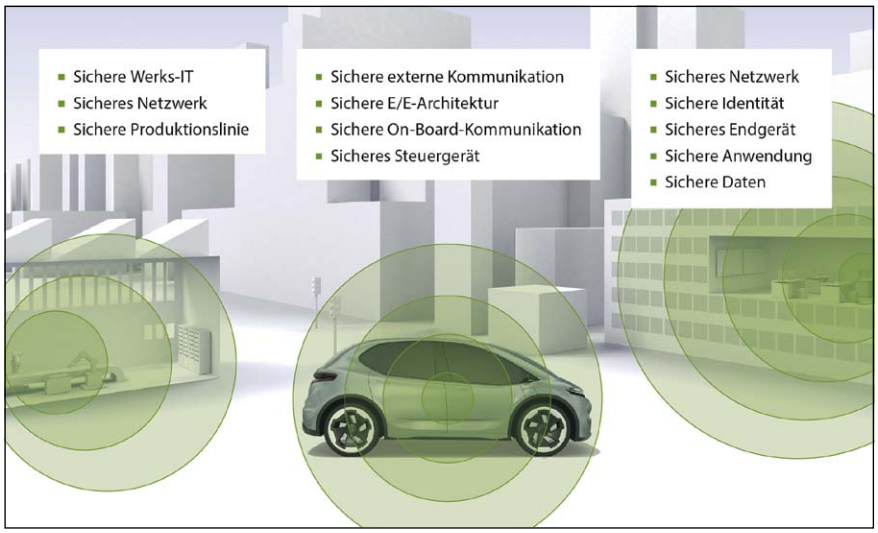

Bild 3. Ein wirksamer Schutz erfordert ein mehrschichtiges Security-Konzept mit mehreren Verteidigungslinien. Der Defense-in-Depth-Ansatz wird dabei nicht nur auf das Fahrzeug, sondern auch auf das vernetzte SDV-Ökosystems angewendet. (Bild: ETAS)

Fahrzeug. Ohne permanente wirksame Absicherung gegen Cyberangriffe, unerlaubten Zugriff und Manipulation wird das SDV nicht erfolgreich bestehen. Gleichwohl orientiert sich Security für das SDV an bekannten Security-Grundprinzipien – muss diese aber viel weitreichender auf neue, elaborierte Art umsetzen:

1. Defense in Depth

Für das Software-definierte Fahrzeug bedarf es in Zukunft mehrschichtiger »Verteidigungslinien« – nicht nur für die Fahrzeuge selbst mit ihren neuen stärker zentralisierten und Zonen-basierten E/E-Architekturen, sondern auch für das SDV-Ökosystem, von der Produktion bis hin zu allen vernetzten Backend-Systemen (**Bild 3**).

Im Software-definierten Fahrzeug muss dieser Defense-in-Depth-Ansatz vor allem die verschiedenen Ebenen der Softwarearchitektur betrachten. Mit Blick auf die gesamte Übertragungskette von Daten zwischen einzelnen Anwendungen lassen sich dann wirksame Security-Maßnahmen integrieren. Zugriffskontrollsysteme und Berechtigungsmanagement müssen dabei allumfassend und sinnvoll zusammengestellt sein – und sowohl die Authentisierung und Autorisierung von Komponenten und Usern als auch die Absicherung und Separierung der Kommunikation mit einbeziehen. Bereits bekannte und etablierte Mechanismen finden dabei selbstverständlich weiterhin Verwendung: Hardware-Security-Module (HSM), Secure Boot, Sichere Onboard-Kommunikation (SecOC), Intrusion-Detection-Systeme (IDS) etc.

2. Security by Design

Das Software-definierte Fahrzeug ermöglicht einen permanenten Software-Entwicklungszyklus über die Lebensspanne des Fahrzeugs hinweg. Cybersecurity für das SDV muss daher über Start-of-Production (SOP) hinaus zum festen Bestandteil dieses kontinuierlichen Entwicklungs- und Updatezyklus der Software werden. Designprinzipien wie Bedrohungsanalysen mit anschließender Risikobewertung (Threat Analysis and Risk Assessment TARA), Secure-Coding-Richtlinien und Security Testing müssen immer wiederkehrend im Prozess der Softwareentwicklung verankert sein.

Im eigentlichen Designprozess der E/E-Architektur des SDV sind zudem zwei Punkte maßgeblich: Zum einen sind grundlegende Security-Maßnahmen verpflichtend umzusetzen (Security by Default), in die Anforderungen an Kommunikationskanäle und Komponenten einzubeziehen und bei der Auswahl der Hardware zu berücksichtigen – etwa durch Integration von Hardware-Security-Modulen in Vehicle Computer und Zonencontroller. Zum anderen gilt es, der sich weiterentwickelnden Gefahrenlandschaft per Krypto-Agilität zu begegnen. Das heißt, die verwendeten kryptographischen Algorithmen müssen Update-fähig sein, zum Beispiel auf höhere Schlüssellängen oder gar post-quantum-sichere Algorithmen hin, und Security-Maßnahmen wie fahrzeuginterne Angriffserkennung und Identity-and-Access-Management (IAM) müssen flexibel und skalierbar gegen künftige neue Angriffe aufrüstbar sein [3].

3. Kontinuierliches Risikomanagement

Das Software-definierte Fahrzeug der nahen Zukunft verlangt mehr denn je nach Managed Security über seinen kompletten Lebenszyklus und die gesamte vernetzte Flotte hinweg – von der Angriffserkennung über die Response bis zur Prävention. Ziel muss sein, entlang der stetigen Weiterentwicklung und Erweiterung der software-basierten Features und Funktionen im SDV ein adäquates Security-Level zu definieren und dessen kontinuierliche Nachjustierung zu ermöglichen. Dabei wird das SDV idealerweise integraler Teil einer flottenweiten Angriffserkennung und -abwehr (Intrusion Detection & Prevention Solution, IDPS), die Cyberattacken oder Schwachstellen identifiziert, analysiert und deren Ausbreiten auf die Flotte verhindert [4].

Angriffe oder Schwachstellen, die bereits während der Softwareentwicklung Eingang in den Code finden und im weiteren Entwicklungsprozess nicht entdeckt werden, können so noch beim Softwarebetrieb durch die verteilte Angriffserkennung im Fahrzeug identifiziert werden (**Bild 4**). Über ein Vehicle Security Operations Center (VSOC) im Backend werden solche potenziellen Angriffe und Schwachstellen

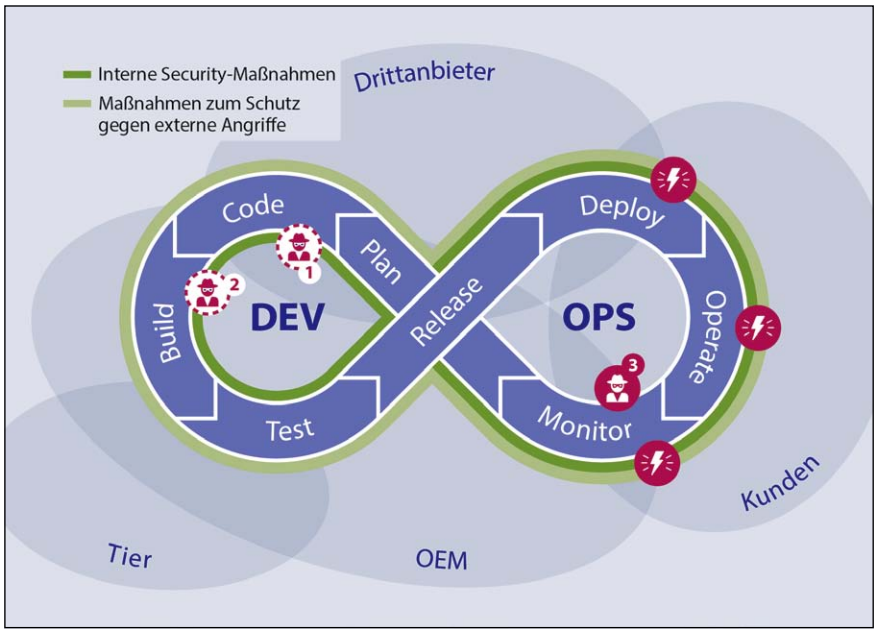

Bild 4: Security-Maßnahmen müssen den gesamten DevOps-Zyklus begleiten – Schwachstellen, die bereits während der Softwareentwicklung Eingang in den Code (1) finden und im weiteren Entwicklungsprozess unentdeckt bleiben (2), können so noch im Softwarebetrieb per Angriffserkennung im Fahrzeug (3) identifiziert werden. (Bild: ETAS)

dann flottenweit aggregiert, analysiert und unmittelbar in Handlungsempfehlungen übersetzt. Diese fließen als kontinuierliches Feedback zurück in die Entwicklung des verantwortlichen OEMS, Flottenbetreibers oder Softwareanbieters, der sodann Gegenmaßnahmen implementiert und über sein Software-Update-Managementsystem (SUMS) per Firmware over-the-air (FOTA) flottenweit ausrollt – die »Abwehrkräfte« des SDV werden so stetig gestärkt.

Gleichzeitig müssen auch alle Prozesse, angefangen bei Entwicklung und Ausbringen der Software-Applikationen bis hin zur Schwachstellenbehebung und Response, Ende-zu-Ende-abgesichert und kontinuierlich verbessert werden – einerseits um auszuschließen, dass manipulierte Software überhaupt erst ins Fahrzeug oder sein SDV-Ökosystem gelangt und andererseits, um im Ernstfall eine schnelle Reaktion zu gewährleisten. Einen Source Code zu verwenden, ohne seine Herkunft zu kennen oder seine Integrität zu schützen, wäre ebenso fahrlässig, wie einen »Zero-Day Exploit«, eine vormals unbekannte Schwachstelle, tagelang im Auto zu belassen, ohne ihn zu patchen.

Security als Key Enabler

Die Transformation hin zum Software-definierten Fahrzeug hat bereits begonnen. Doch mit dem SDV in seinem Ökosystem werden die Angriffsfläche für Cyberattacken und das Schadenspotenzial um ein Vielfaches anwachsen. Cyberkriminellen bietet das exzellente Chancen, ihre lukrativen Geschäfte rund um Ransomware, Malware-as-a-Service, illegalen Datenhandel etc. auf ein neues »Spielfeld« auszuweiten. Fahrzeugherstellern, Flottenbetreibern und Mobility-Service-Providern im neuen SDV-Markt drohen gravierende Folgen: Betriebsausfälle oder Inoperabilität der Flotte, Lösegeldzahlungen oder Wiederherstellungskosten, Reputationsverlust und Haftungsansprüche. Nur diejenigen, die der Cybersicherheit des SDVs und seines vernetzten Ökosystems einen hohen Stellenwert zuweisen, werden hier bestehen und ihre neuen auf Software basierenden Geschäftsmodelle erfolgreich etablieren.

Cybersecurity wird zum Key Enabler des Software-definierten Fahrzeugs. Einzellösungen werden hierzu nicht reichen. Stattdessen gilt es, Security-Maßnahmen – nicht allein in technischer Hinsicht, sondern insbesondere auch in Gestalt Security-gerechter Organisation und Prozesse – unter einer ganzheitlichen Security-Strategie für das SDV und sein Ökosystem zu bündeln und auf allen Systemebenen sowie über die gesamte SDV-Lebensspanne hinweg entlang des wiederkehrenden DevOps-Zyklus wirksam werden zu lassen. Sowohl OEMs als auch Zulieferer müssen dabei schnell reagieren und bereits heute anfangen, solchermaßen holistische Security-Strategien zu definieren und für die nächste Fahrzeuggeneration umzusetzen. Nur so kann der DevOps- zu einem DevSecOps-Zyklus werden. ih

Literatur

[1] Bernd Oswald: Sitzheizung for free - Hacker untergraben Abo-Modell von BMW, unter: https://www.br.de/nachrichten/netzwelt/sitzheizung-for-free-hacker-untergraben-abo-modell-von-bmw,TCDjrVQ

[2] Heise online: Fahrzeugsicherheit - Wenn das Auto ein Teil des Internets wird, unter: https://www.heise.de/newsticker/meldung/Fahrzeugsicherheit-Wenn-das-Auto-ein-Teil-des-Internets-wird-4565362.html

[3] Ramona Jung: Software-definierte Fahrzeuge - Zonale E/E-Architekturen wirksam absichern, Hanser automotive 3/2022.

[4] Jan Holle et al: Intrusion detection and prevention solution - Immune system for connected vehicle fleets, Whitepaper Escrypt 09/2021, unter: https://www.escrypt.com/sites/default/files/downloads/escrypt-whitepaper-idps.pdf

Carina Böttcher

verantwortet als Product Field Manager die Professional Security Services bei Escrypt, der Cybersecurity-Marke von ETAS.

Dr. Thomas Wollinger

ist als Vice President von ETAS verantwortlich für das Portfolio Management Cybersecurity Solutions unter der Marke Escrypt.