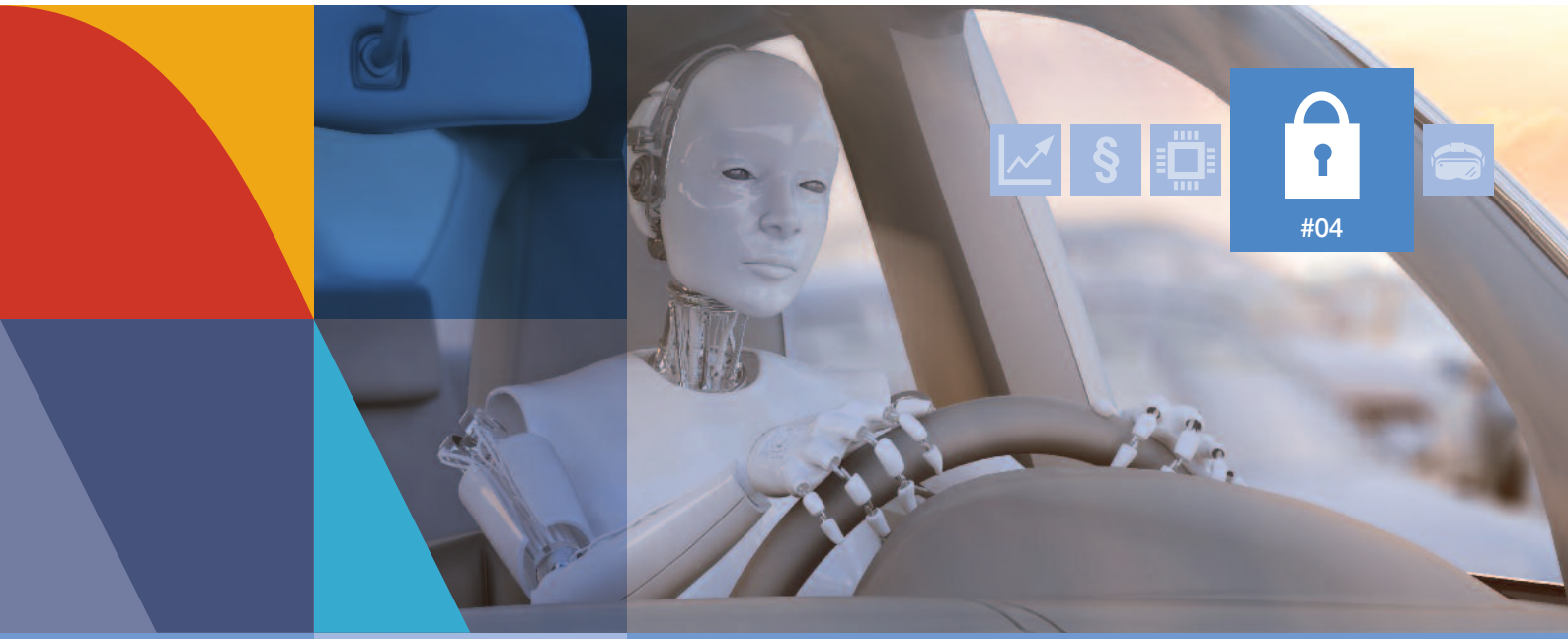
NTT DATA
Trusted Global Innovator



WHITEPAPER-SERIE AUTONOMES FAHREN

#04 Sicherheit

NTT DATA Deutschland GmbH

Inhaltsübersicht

1. Grußwort von Kai Grunwitz, Senior Vice President EMEA, NTT Security

Liebe Leserinnen und Leser,

mit dem zunehmenden Reifegrad des autonomen Fahrens wird Security noch stärker in den Fokus der Öffentlichkeit rücken. Der kommende Ausbau von LTE-V, 5G, Car2X- und Car2Car-Kommunikation wird zudem neue Security-Themen auf die Agenda bringen, mit denen sich alle Beteiligten – ob Fahrzeughersteller, Regierungs- und Nichtregierungsorganisationen oder Security-Anbieter – beschäftigen müssen. Insbesondere die Politik ist gefragt, hier die notwendigen Rahmenbedingungen so schnell wie möglich zu schaffen, um erstens die Entwicklung im Bereich autonomes Fahren und Fahrzeug-Security weiter voranzutreiben und zweitens diese auch sicher zu gestalten.

Jedoch ist es nicht empfehlenswert, abzuwarten, bis die offiziellen globalen und lokalen Sicherheitsrichtlinien für autonomes Fahren in Kraft treten. Vielmehr sollten Fahrzeughersteller und Zulieferer das Thema Sicherheit bereits heute anpacken, um dann im Wettbewerb die Nase vorn zu haben, wenn es in punkto Security »ernst« wird, also entsprechende Gesetze, Richtlinien und Standards vorliegen. Gefragt sind hier nicht einzelne Sicherheitsmaßnahmen, sondern ein stimmiges Gesamtkonzept.

Ein Beispiel dafür ist der Standard ISO/SAE 21434 „Road vehicles – Cybersecurity engineering“, der ab 2021 verpflichtend für die Zulassung von Fahrzeugen werden soll. Aktuell ist die Norm noch im Draftstatus. Doch sobald der Standard final ist, müssen OEMs schnell entsprechend handeln. Offen ist noch die Frage, ob die neue Cyber-Security-Norm auch Zulieferer betrifft. Denn es ist davon auszugehen, dass OEMs die neuen Verpflichtungen an ihre Zulieferer »durchreichen«.

Kurzum: Nicht nur OEMs, auch Zulieferer sollten in Sachen Security jetzt aktiv werden, und zwar mit Konzept. In diesem Whitepaper erfahren Sie mehr über die aktuell größten Sicherheitsgefahren, den derzeitigen Stand der gesetzlichen Rahmenbedingungen sowie Ansätze, um Sicherheit in die DNA der Fahrzeugentwicklung zu implementieren – und wie Sie NTT DATA gemeinsam mit NTT Security bei all dem unterstützen kann.

Das vorliegende Whitepaper stammt aus der Feder von NTT Security, dem Schwesterunternehmen von NTT DATA mit weltweit mehr als 1.500 Sicherheitsexperten und sieben Zentren für Forschung und Entwicklung rund um den Globus. Damit erhalten Sie hier Informationen aus erster Hand.

Ich wünsche Ihnen eine anregende Lektüre

Kai Grunwitz

2. Vernetztes Fahrzeug: Ziel von Hackerangriffen

Status quo. Mit dem Aufkommen von Smartphones 2008 sowie dem damit verbundenen Ausbau des mobilen Datennetzes war es nur eine Frage der Zeit, bis das Internet auch in Fahrzeugen Einzug halten würde. Dementsprechend bietet heutzutage nahezu jeder Fahrzeughersteller digitale Features in seinen Fahrzeugen an: angefangen von USB, Bluetooth und WLAN über Infrarot-, Laser- oder Radarsensoren bis hin zur Internetfähigkeit des Fahrzeuges selbst durch integrierte Datenmodule. Fahrzeuge erhalten somit permanent Informationen von externen Quellen.

Angriffsgründe und ihre – schlimmstenfalls tödlichen – Folgen. Allerdings werden Fahrzeuge dadurch auch mögliche Ziele von Hackerangriffen. Die Motivation für solch einen Angriff kann verschiedene Gründe haben: Zum Beispiel kann ein Hacker versuchen, über Softwaremanipulation sein Fahrzeug aufzubessern (zu „tunen“), um mehr Leistung zu erhalten, den Tachostand zu manipulieren oder um die Abriegelung einer maximal möglichen Geschwindigkeit abzuschalten. Ein weiterer Grund kann sein, dass sich ein Hacker über Fahrzeugsysteme unerlaubten Zugang verschaffen will, um das Fahrzeug zu entwenden ohne Einbruchspuren zu hinterlassen. Versucht jedoch ein Hacker, sicherheitsrelevante Systeme wie Lenkung oder Bremsen zu übernehmen, kann das im schlimmsten Fall zu tödlichen Unfällen führen. Anders formuliert: Für eine Privatperson ist es zwar ärgerlich, wenn das Smartphone gehackt wird und für ein Unternehmen kann dies einen hohen wirtschaftlichen Schaden nach sich ziehen. Doch ein Hackerangriff auf ein Fahrzeug kann eine echte Gefahr für Leib und Leben bedeuten.

Deshalb sind hier die Hersteller von heute teilautomatisierten und in Zukunft vollautomatisierten Fahrzeugen in der Pflicht, weiterhin alles für eine größtmögliche Cyber-Sicherheit zu tun.

3. Bisherige Sicherheitsmaßnahmen nicht ausreichend

Derzeit wird versucht, die bestehenden Fahrzeugarchitekturen möglichst gut gegen Angriffe abzusichern. Dies gelingt allerdings nur partiell. Gründe hierfür gibt es mehrere.

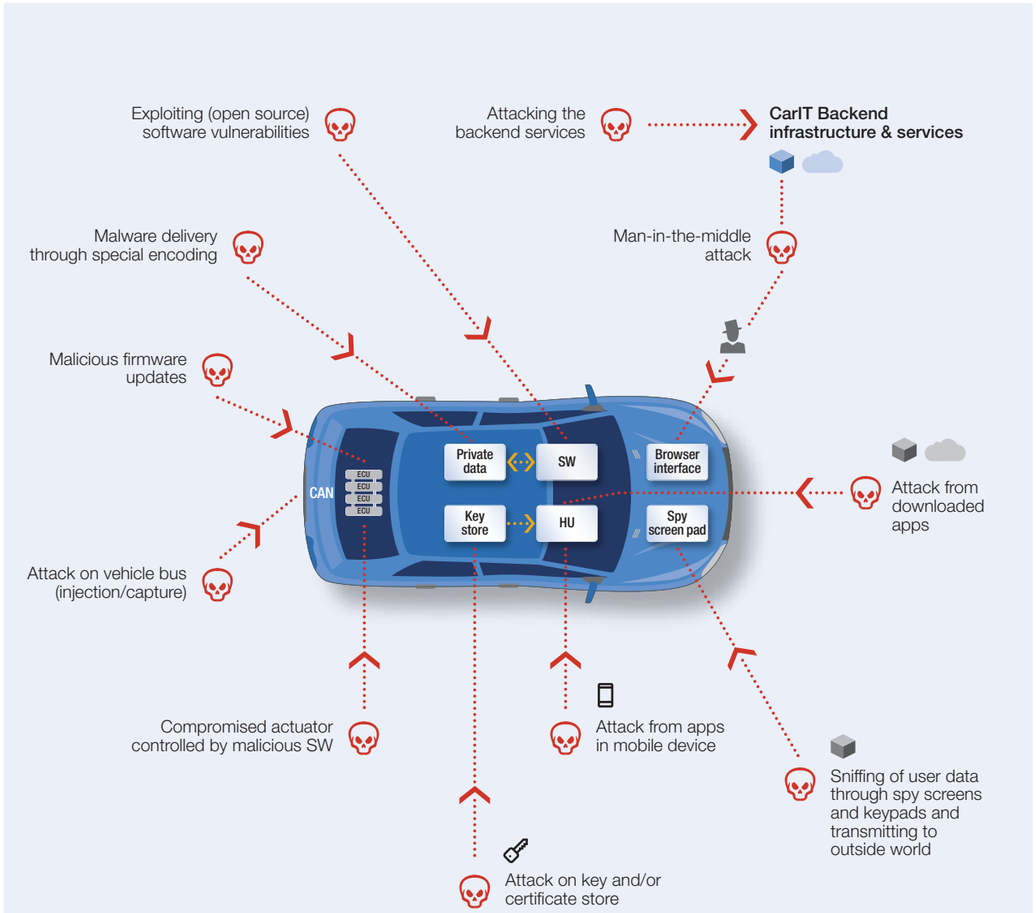
- **1. Funktionale Sicherheit ist nicht gleich Informationssicherheit:** Die derzeitige Fahrzeugarchitektur ist meist historisch gewachsen. Dabei standen stets die Funktionsorientierung der Systeme und deren funktionale Sicherheit (Safety) im Vordergrund und nicht die Informationssicherheit (Security). Fahrzeugsysteme waren ursprünglich gar nicht darauf ausgelegt, Schutz vor Cyber-Angriffen zu bieten.

- **2. Die Gefahr lauert auch im Fahrzeug:** Derzeitige Schutzmaßnahmen beschränken sich darauf, den Zu- und Abfluss der Daten in und aus dem Fahrzeug zu kontrollieren (Perimeter-Schutz). Dabei wird aber nicht überprüft, wie die Daten sich im Fahrzeug selbst verhalten oder welche Aktionen sie dort ausführen. So kann es passieren, dass ein verpacktes Datenpaket die Firewall des Fahrzeuges passiert, dann im Fahrzeug entpackt wird und dort Schaden anrichtet. Gelöst werden kann dieses Problem mit einem Gateway-Punkt, über den alle Daten laufen. Die Steuergeräte und Infotainment-Systeme kommunizieren somit nicht mehr direkt, sondern über einen zentralen Punkt, der den Traffic überwacht.

- **3. Fehlende Kontrolle:** Fahrzeughersteller haben nur eine eingeschränkte Kontrolle über Daten, welche von externen Quellen in das Fahrzeug eingespielt werden. Dies gilt zum Beispiel für Daten, welche über die USB- oder Bluetooth-Verbindung mit einem Smartphone in das Fahrzeug gelangen. Dementsprechend ist es für kommende Generationen von vernetzten und autonomen Fahrzeugen essenziell, IT-Sicherheitskonzepte gegen Hackerangriffe zu entwickeln.

4. Die größten Gefahren im Überblick

Viele Angriffspunkte – vor allem in den fahrzeugeigenen Systemen. Die IT-Systeme eines modernen Fahrzeugs sind vernetzt – untereinander und mit der Außenwelt. Während heute die meisten Gefahren für Connected Cars aus der Verknüpfung mit der Außenwelt resultieren, liegen die Sicherheitsrisiken für autonome Fahrzeuge vor allem in den Verbindungen der fahrzeugeigenen Systeme untereinander. Denn: Autonome Fahrzeuge müssen auch ohne Verbindung zum Backend funktionieren – eben autonom. Dies macht es für Hacker besonders interessant, die internen Security-Schwachstellen der Fahrzeuge zu attackieren.



Übersicht der Angriffspunkte eines vernetzten Fahrzeuges. Bildquelle: NTT

4.1 Angriffe über Media-Schnittstellen

Moderne Fahrzeuge verfügen über zahlreiche Media-Schnittstellen, zum Beispiel Bluetooth, USB oder WLAN-Hotspots; Nutzer können damit telefonieren, Musik streamen, auf Facebook chatten oder E-Mails lesen; über diese Zugänge sind Angriffe mit einfachen Mitteln und Standard-Tools möglich, beispielsweise indem Schadcode durch infizierte Media-Dateien eingeschleust oder durch Anwendungen im Fahrzeug heruntergeladen wird. Das Patching der Media-Komponenten wird bestenfalls im Rahmen einer Inspektion durchgeführt. Die Fahrzeughersteller verlassen sich hier bisher auf die Services der jeweiligen Provider.

4.2 Beeinflussung von Fahrzeugsensoren und Car2X-Kommunikation

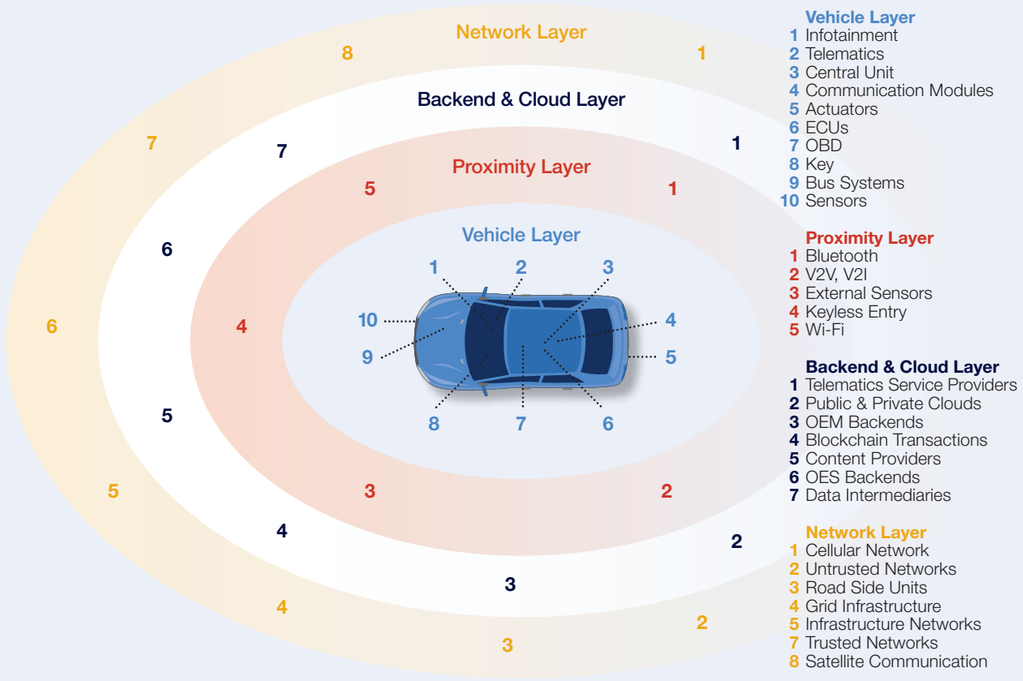
Fahrzeugsensoren, beispielsweise für Abstandsregelung oder Bremsassistenten, sind aktuell extern nur mit großem Aufwand zu beeinflussen, etwa durch das Senden von Störsignalen. Ähnliches gilt für Komponenten der Car2X-Kommunikation, zum Beispiel Ampeln, Verkehrszeichen oder andere Fahrzeuge. Dafür ist hier das Gefahrenpotenzial besonders hoch, zum Beispiel indem eine Vollbremsung ausgelöst oder unterbunden wird. Dieser Angriffssektor wird vor allem aufgrund der wachsenden Bedeutung der Car2X-Kommunikation wichtig, weil die Beeinflussung eines Fahrzeugs sich auch auf andere auswirkt, etwa wenn miteinander kommunizierende Autos Kolonne fahren oder Daten einer Ampel vom Fahrzeug falsch interpretiert werden. Die Sicherung dieser Systeme, etwa durch gehärtete Interfaces und die Kombination von Security und Safety, gewinnt daher an Bedeutung.

4.3 Angriffe bei physischem Zugriff auf das Fahrzeug

Wer physischen Zugriff auf ein Fahrzeug hat, kann Bus-Systeme oder Steuergeräte (ECUs) analysieren und verändern oder schlimmstenfalls über das Gateway des Fahrzeugs auf die Backend-Systeme des Herstellers zugreifen. Diese Art des Zugriffs auf Fahrzeugsteuergeräte und Bus-Systeme lässt sich nicht unterbinden. Durch den Einsatz von IP-Protokollen im Fahrzeug ist der Angriff ohnehin einfacher als über Bus-Systeme wie CAN-Bus oder FLEX-Bus. Fahrzeughersteller können bei physischem Zugriff keine vollständige Sicherheit realisieren, da gewisse Schnittstellen im Fahrzeug bereitgestellt werden müssen. Umso wichtiger ist die sichere und authentifizierte Kommunikation zwischen den Steuergeräten und dem Bus-System beziehungsweise dem IP-Netzwerk im Fahrzeug.

4.4 Angriffe auf Backend-Systeme via Web

Fahrzeugsteuergeräte und Head Units verschiedener Hersteller tauschen bereits heute umfassend Daten mit Hersteller- und Internet-Services aus, beispielsweise über Standort, Fahrziele, offene Fenster und Türen, Service-Daten oder Schadensereignisse. Entsprechende Informationen können oft schon über Fahrzeug-Apps auf Smartphones und Webbrowser abgerufen werden. Auch damit entsteht ein zentraler Angriffspunkt auf Fahrzeuge. Aus Sicherheitssicht besteht hier allerdings der Vorteil, dass diese Systeme bei den meisten Herstellern als „klassische“ IT-Systeme betrieben werden, die den IT-Prozessen unterliegen und damit beispielsweise regelmäßig gepatcht werden. Die Anwendungen haben damit natürlich die gleichen Probleme wie andere IT-Anwendungen; ein kontinuierliches Security Testing und eine risikoadäquate Architektur sind daher unerlässlich.



Verschiedene Angriffsreichweiten

■ **„Vehicle Layer“.** Neben unterschiedlichen Angriffswegen gibt es auch verschiedene Angriffsreichweiten. Angriffe auf das „Vehicle Layer“ beziehen sich direkt auf das Fahrzeug. Anders formuliert: Das Fahrzeug ist das direkte Ziel eines Angriffs. Es wird versucht, über verschiedene Wege das Fahrzeug zu kompromittieren. Dafür ist teils eine physische Präsenz am Fahrzeug nötig.

■ **„Proximity Layer“.** Angriffe auf die „Proximity Layer“ sind Angriffe auf die nähere beziehungsweise in der näheren Umgebung des Fahrzeugs. Es wird versucht, Technologie wie Wi-Fi oder Bluetooth zu kompromittieren und so Zugang zu Fahrzeugsystemen zu erhalten.

■ **„Backend & Cloud Layer“.** In der „Backend & Cloud Layer“ wird das Fahrzeug nicht unmittelbar angegriffen, sondern dessen Backend-Infrastruktur beim Hersteller oder bei den Service Providern. Auch hier kann versucht werden, entweder über diese Wege Zugriff auf Fahrzeugsysteme zu erhalten oder aber Daten aus dem Backend auszuspähen (zum Beispiel Daten über den Fahrer beim Service Provider „Versicherung“).

■ **„Network Layer“.** In der „Network Layer“ werden weitgespannte Netzwerke ausgenutzt. Dabei muss nicht immer ein bestimmtes Fahrzeug das Ziel eines Angriffs sein, sondern es kann auch versucht werden, über Scans potenzielle Opfer zu lokalisieren.

Übersicht über die verschiedenen Angriffsreichweiten. Bildquelle: NTT

5. Neue Rahmenbedingungen für autonome Fahrzeuge

■ 5.1 Neue Geschäftsmodelle

Zusätzlich zu den Anforderungen an die bisherige Fahrzeugarchitektur und IT-Sicherheitsmaßnahmen für diese ändern sich durch vernetzte Fahrzeuge auch die Rahmenbedingungen. So kann man die Entstehung von neuen Geschäftsmodellen beobachten, sowohl bei Herstellern, Zulieferern und verschiedenen Service Providern, teils auch in Kombination zusammen. Zum Beispiel ist es heute schon möglich, in Fahrzeugen mit integrierter SIM-Karte Datenpakete bei Mobilfunkanbietern zu buchen und diese über den WLAN Hotspot des Fahrzeugs mit einem Tablet oder Laptop zu nutzen. Es ist abzusehen, dass solche zahlungspflichtigen Extradienste mehr und mehr zunehmen werden (pay-per-use-Prinzip). Weitere Dienste könnten zum Beispiel das Freischalten von Extra-PS für den Wochenendausflug oder das zeitweilige Zubuchen von Assistenzsystemen für eine lange Autobahnfahrt sein.

■ 5.2 Neue Rechtsgrundlagen

Außerdem hat auch die Politik erkannt, dass eine tragfähige Rechtsgrundlage für autonomes Fahren und Connected Cars geschaffen werden muss, und ist inzwischen bei der Entwicklung von entsprechenden gesetzlichen Richtlinien.

USA. In den USA sind das:

- SPY CAR Act für IT-Security- und Privacy-Standards für Fahrzeuge
- Autonomous Vehicle Privacy Protection Act für den Schutz von Kunden- beziehungsweise Fahrerdaten.
- NHTSA. Die National Highway Traffic Safety Administration (NHTSA) hat Richtlinien für IT-Sicherheit in Fahrzeugen erstellt.
- NIST. Das National Institute of Standards and Technology (NIST) hat ein Security Framework entwickelt, welches auch für Fahrzeuge gilt.

Europäische Union.
Auch in der EU gibt es neue Richtlinien für dieses Thema:

- DSGVO. Die Datenschutzgrundverordnung (DSGVO) setzt seit 2018 neue Richtlinien für den Schutz von personenbezogenen Daten fest.
- ENISA. Die European Union Agency for Network and Information Security (ENISA) hat Guidelines für Automotive Cyber Security veröffentlicht.
- UN-TF CS/OTA. Die UN Task Force on Cyber Security and OTA issues (UN-TF CS/OTA) arbeitet an einem Standard für Sicherheit beim autonomen Fahren und bei Over-the-Air-Updates.

Japan. Und in Japan gibt es vom Ministerium für innere Angelegenheiten und Kommunikation (MIC) die „Automotive Cyber Security“-Richtlinie.

■ 5.3 Neue Standards

Auch verschiedene Standardisierungsorganisationen haben sich des Themas angenommen und sind dabei, passende Standards zu schaffen:

ISO 26262. Die Internationale Standardisierungsorganisation (ISO) hat schon 2009 ISO 26262 herausgebracht. Dieser Standard fokussiert sich aber auf funktionale Sicherheit (Safety) und ist für Automotive Cyber Security nur bedingt geeignet.

ISO/SAE 21434. In Abstimmung mit der EU wird von der United Nations Economic Commission for Europe (UNECE) eine Zertifizierung für ein „Cyber Security Management System“ (CSMS) für Fahrzeuge erarbeitet, die nach den aktuellen Vorschlägen ab 2021 verpflichtend für die Typzulassung von Fahrzeugen sein soll. Mit der ISO/SAE 21434 soll dazu ein Standard für die Automobilentwicklung geschaffen werden. Dieser umfasst den gesamten Lebenszyklus von Fahrzeugen, um die Security von der Entwicklung über die Produktion bis zum Zeitpunkt nach dem Verkauf sicherzustellen. Aktuell befindet sich der Standard noch im Draft-Modus.

NTT unterstützt OEMs bei der Umsetzung dieses neuen Standards mit einem umfassenden Service-Portfolio aus den Bereichen Governance, Risk & Compliance, Sicherheitsmanagement, sichere Entwicklungsprozesse, Car Security und Produktions-Security.

SAE J3061. Auf dieser Basis hat der Verband der Automobilingenieure (SAE) 2016 den Standard SAE J3061 entwickelt, welcher speziell für Cyber Security in Fahrzeugen ausgelegt ist. Derzeit gibt es ein Mapping zwischen ISO 26262 und SAE J3061, um einen homogenen Standard zu erhalten.

Verschiedene ETSI-Standards. Das Europäische Institut für Telekommunikationsnormen (ETSI) hat mehrere Standards für verschiedene Bereiche herausgebracht, welche meist zwar nicht ausschließlich für Fahrzeuge gedacht sind, aber Technologien betreffen, welche in Fahrzeugen verbaut sind. Das sind zum Beispiel Standards unter dem Oberbegriff „Automotive Radar“, welche sich mit der Standardisierung von Radartechnologie für weite und für kurze Strecken beschäftigen – in der Automobilindustrie meist als „Adaptive Cruise Control“ (ACC) beziehungsweise „Parksensoren“ und „Notbremsassistent“ bezeichnet.

Weitere Standards für Cyber-Sicherheit. Des Weiteren gibt es eine ganze Reihe Standards, welche sich mit Cyber Security beschäftigen und sich dabei auch um eine Annäherung an das amerikanische Pendant Institute of Electrical and Electronics Engineers (IEEE) bemühen. Diese Standards beschäftigen sich zum Beispiel mit der Kommunikation zwischen zwei Fahrzeugen und einem Austausch von Zertifikaten und Signaturen zwischen diesen oder der Entwicklung eines Trust-Modells für Car2Car-Kommunikation.

6. Security by Design – Sicherheit beginnt bei der Entwicklung

Ganz von vorn anfangen. Um ein lückenlos sicheres System zu erschaffen, muss bei der IT-Sicherheit von autonomen Fahrzeugen noch einmal bei null angefangen werden. Bisher wurden IT-Systeme an die Fahrzeuge angepasst. Mit der zunehmenden Vernetzung der Fahrzeuge werden die Systeme jedoch so umfangreich, dass eine solche Anpassung zu komplex und fehleranfällig werden würde. Wenn sich die IT-Systeme mit Fahrfunktionen vernetzen oder gar die Steuerung des Autos übernehmen, wird das Thema noch ernster. Bei einem nicht-systematisch entwickelten, angepassten IT-System wäre hier die Gefahr viel zu groß, dass Hacker die Kontrolle über das Fahrzeug übernehmen und Menschenleben gefährden.

Komplett umdenken. In der Fahrzeugentwicklung muss daher komplett umgedacht werden. Um die bestmögliche Sicherheit zu garantieren, muss es in Zukunft heißen: IT und Technik sind gleichberechtigt. In der Praxis bedeutet das: Für die autonome Fahrzeugentwicklung muss der Grundsatz „Security by Design“ gelten.

Das Fahrzeug als System. Das Fahrzeug wird dabei als Gesamtsystem betrachtet, das aus Technik- und IT-Untersystemen besteht, die miteinander zu verknüpfen sind. Dazu müssen Ingenieure und IT-Entwickler von Anfang an eng kooperieren. Nur durch eine solche bereichsübergreifende Zusammenarbeit lassen sich Sicherheitslücken und Fehler bestmöglich ausschließen.

Fahrzeugentwicklung der Zukunft. Fazit: Die IT darf nicht länger „im Nachgang“ für ein fertiges Fahrzeug entwickelt werden, sondern muss gleichzeitig mit der Fahrzeugtechnik entworfen werden. Wie Fahrzeughersteller ihre Produktentwicklungsprozesse umstellen können, um diesen Anforderungen gerecht zu werden, erfahren Sie im fünften Teil unserer Whitepaper-Serie zum autonomen Fahren. Diese widmet sich gänzlich dem Thema „Fahrzeugentwicklung der Zukunft“ und dem Konzept des Model-Based-Systems-Engineering (MBSE) – der Lösung für eine reibungslose Kooperation von Ingenieuren und IT-Teams.

7. Die Umsetzung: Defense in Depth

Security by Design ist lediglich ein Ansatz, jedoch kein umfassendes Konzept. Eine Möglichkeit, Security by Design umzusetzen, ist das Konzept „Defense in Depth“.

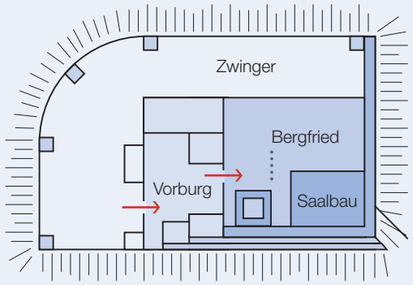
Umfassendes Sicherheitskonzept. Für Defense in Depth werden verschiedene Maßnahmen – auch Abwehr- oder Verteidigungslinien genannt – kombiniert, um Risiken für einen Angriff auf die IT zu minimieren. Maßnahmen können sowohl IT-Maßnahmen sein, also zum Beispiel der Einsatz von Sicherheitssystemen für Verschlüsselung, Virenschutz, Berechtigungsmanagement etc., oder auch organisatorische Maßnahmen wie das Schulen von Mitarbeitern bezüglich Security Awareness oder das Aufstellen von entsprechenden Dienstanweisungen. Wichtig ist auch, dass für einen erfolgreichen Defense-in-Depth-Ansatz alle Beteiligten mitwirken müssen: Hersteller, Provider, Integratoren, Externe Ressourcen, IT-Mitarbeiter und Mitarbeiter aus anderen Bereichen.

Einheitliche Rahmenbedingungen für autonome Fahrzeuge aktuell in Arbeit

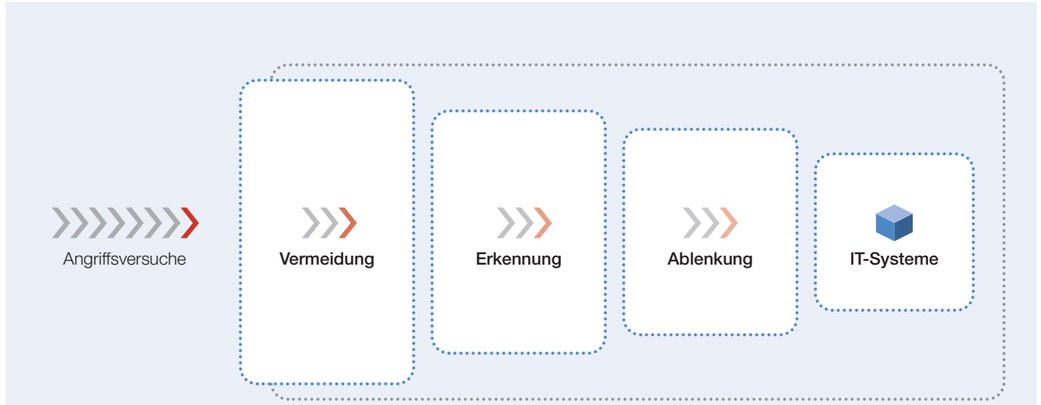
Obwohl kein Zweifel daran besteht, dass Sicherheit einer der zentralen Faktoren für die flächendeckende Einführung autonomer Fahrzeuge ist, gibt es dafür bislang noch keine umfassenden Cyber-Security-Konzepte. Der Grund: Die Hersteller sind noch nicht so weit und vor allem fehlen bislang einheitliche Rahmenbedingungen. Die Internationale Organisation für Normung (ISO) und die Society of Automotive Engineers (SAE) arbeiten an einer gemeinsamen Norm (ISO 21434), die Mindestanforderungen an die Sicherheitskonzepte für autonome Fahrzeuge festsetzt. Dafür haben beide Institute eigenständige Skizzen erstellt, die nun noch zusammengeführt werden müssen. Es wird geschätzt, dass dieser Prozess noch zwei bis drei Jahre in Anspruch nehmen wird.

7.1 Verschiedene Ansätze

1. Aus dem Mittelalter. Defense in Depth ist keine Erfindung der heutigen IT. Das Konzept kommt vielmehr aus dem Militär und wurde schon im Mittelalter angewandt. Dort wurden Städte und Burgen nach dem Defense-in-Depth-Konzept aufgebaut:
Die äußerste Abwehrlinie war hier ein Graben, dann kam die erste Mauer mit Türmen, dann die Vorburg und zum Schluss die Hauptburg mit dem Bergfried als letztem Rückzugsort. Zwischen den einzelnen Bereichen gab es jeweils nur einen Zugang durch ein Tor, wo kontrolliert wurde, wer hineinkommt und wer hinausgeht. Ein Angreifer konnte nicht gleich in das Innerste der Burg vordringen, sondern musste nach und nach die einzelnen Verteidigungsanlagen überwinden. Das gleiche Prinzip gilt noch heute in der IT.



Schematischer Aufbau einer Burg am Beispiel Burg Oberlauda. Um die Burg gab es einen 18 Meter tiefen Graben mit einer Mauer. Die Wehrtürme waren auf der Talseite der Burg gebaut. Auf der Bergseite der Burg befanden sich schließlich gut geschützt Saalbau und Bergfried. | Eigene Abbildung in Anlehnung an Friedrich Wilhelm Krahe „Burgen des deutschen Mittelalters“ (Flechsig Verlag, Würzburg, 2000)



Defense-in-Depth-Ansatz.

Eigene Abbildung in Anlehnung an Ulf E. Larson und Dennis K. Nilsson
„A Defense-in-Depth Approach to Securing the Wireless Vehicle Infrastructure” (Journal of Networks, 2009, Band 4 und 7)

2. Neuer Ansatz.
Ein anderer Ansatz von Defense in Depth stammt von den schwedischen Wissenschaftlern Dr. Ulf Larson und Dennis Nilsson. Diese beschreiben Defense in Depth als das Zusammenspiel von verschiedenen Stufen oder Vorgehensweisen, um Angreifer abzuwehren. In ihrem Modell gibt es drei Stufen, welche auch in dieser Reihenfolge greifen sollen: Vermeidung (Prevention), Erkennung (Detection) und Ablenkung (Deflection):
Dabei gilt der Grundsatz, so viele Angriffswege wie möglich zu vermeiden. Angriffe, die nicht abgewehrt werden können, deren Schutz zu teuer ist beziehungsweise die Kosten dafür nicht in Relation mit dem Sicherheitsgewinn stehen, sollen zumindest erkannt werden, um dann Maßnahmen treffen zu können. Ablenkung beschreibt das Aufstellen von sogenannten „Honeypots“, also Servern mit nur scheinbar wertvollen Daten wie Adressen und Dokumenten.
Angreifer sollen so auf Systeme gelenkt werden, bei denen sie keinen Schaden anrichten können. Und Sicherheitsexperten haben damit die Möglichkeit, den Angreifer und sein Vorgehen zu studieren.

7.2 Nachteile

Allerdings hat der Defense-in-Depth-Ansatz auch Nachteile – zum Beispiel die Geschwindigkeit: Je mehr Zwischenstationen und Prüfungen durchlaufen werden müssen, desto länger brauchen die Daten von ihrer Quelle zu ihrem Ziel. In Systemen oder Anwendungen, bei denen Zeit ein wichtiger Faktor ist, kann dies zum Problem werden. Dies gilt insbesondere bei Echtzeitanforderungen wie in Connected Cars. Ein weiterer Nachteil sind die Kosten. Mehr Sicherheit heißt in der Regel auch immer zusätzliche Investitionen. Und je mehr Zonen und Verbindungen es gibt, desto mehr Sicherheitskomponenten werden benötigt, um diese abzusichern. Es gilt also Kosten und Nutzen abzuwägen, ob mehr Sicherheitstechnik ab einem bestimmten Level das Sicherheitsniveau noch merklich hebt. Außerdem muss bei diesem Modell Sicherheit von allen Beteiligten gelebt und umgesetzt werden. Das heißt: Alle benötigen das erforderliche Wissen und die entsprechende Security Awareness – eine organisatorische Herausforderung für Unternehmen.

8. Fazit: Jetzt aktiv werden!

Sicherheit braucht Konzept. Es gibt nicht den einen Weg, um Fahrzeuge abzusichern. Vielmehr entsteht ein aus IT-Sicht sicheres Fahrzeug durch ein stimmiges Gesamtkonzept, das sich wiederum aus vielen einzelnen Komponenten und Prozessschritten zusammensetzt, die alle zusammenpassen müssen. Bevor viele der vorgestellten Schutzmaßnahmen im Fahrzeug umgesetzt werden können, bedarf es noch viel Vorarbeit, auf prozessualer wie auf systemseitiger Ebene.

Sicherheit über den gesamten Produktlebenszyklus. Darüber hinaus gilt es, einen Prozess zu definieren, wie IT-Sicherheit über den gesamten Produktlebenszyklus implementiert und umgesetzt werden kann – von den ersten Entwürfen über die Entwicklung, Herstellung und Nutzung bis hin zur Verschrottung. Dabei muss auch beachtet werden, dass sich während des langen Lebenszyklus externe Faktoren unvorhergesehen verändern können. So kann es zum Beispiel sein, dass ein Fahrzeug nicht mehr erreichbar ist, weil der Besitzer die Mobilfunkeinheit abgeschaltet hat, diese defekt ist oder dass genutzte Funktionen nicht mehr zur Verfügung stehen.

Sicherheitsrichtlinien zwingen zum Handeln. Der Bedarf von OEMs nach einem ganzheitlichen Sicherheitsmodell wächst – gezwungenermaßen. Denn Richtlinien von Regierungen oder staatlichen Organisationen in punkto Einhaltung eines Mindeststandards an Sicherheit im Fahrzeug sind bereits in Sicht. Dabei wird es globale Richtlinien geben ebenso wie regionale Standards, welche eine zusätzliche Hürde bei der Einhaltung und Implementierung von Security darstellen.

Jetzt Wettbewerbsvorteile sichern und Kundenvertrauen gewinnen. Es empfiehlt sich daher, dass Automobilhersteller und Zulieferer sich bereits heute Gedanken über die Umsetzung von Security machen, bevor der Druck eines Gesetzes sie dazu zwingt. So lässt sich ein Vorteil gegenüber Wettbewerbern erreichen und auch einem Vertrauensverlust der Kunden (durch einen Angriff) vorbeugen.

9. Unterstützung von NTT DATA – Hand in Hand mit NTT Security

NTT DATA unterstützt seit Jahrzehnten die etablierte Automobil- und Zuliefererindustrie mit integrierten Gesamtlösungen und stellt so ein gut funktionierendes Zusammenspiel von Prozessen und IT-Applikationen sicher. In Sachen Sicherheit arbeitet NTT DATA Hand in Hand mit seiner Konzernschwester NTT Security zusammen. NTT Security ist das auf Sicherheit spezialisierte „Security Center of Excellence“ der NTT Group. Mit „Embedded Security“ ermöglicht NTT Security den Unternehmen der NTT Group die Bereitstellung zuverlässiger Business-Lösungen für die digitale Transformation ihrer Kunden. Weltweit über 1.500 Sicherheitsexperten von NTT Security kümmern sich jährlich um Hunderttausende Sicherheitsvorfälle auf sechs Kontinenten. Gemeinsam bilden NTT DATA und NTT Security ein Team mit einer marktweit einzigartigen Expertise in Automotive Security.

Wenden Sie sich an uns!

- **Autonomes Fahren – Whitepaper-Serie von NTT DATA**

Lesen Sie mehr zum autonomen Fahren.
In unserer Whitepaper-Serie behandeln wir u. a. die folgenden Themen:

- **#01** Entwicklung des autonomen Fahrens
- **#02** Rechtliche und gesellschaftliche Voraussetzungen
- **#03** Technische Voraussetzungen
- **#05** Fahrzeugentwicklung der Zukunft

10. Autor

georg.graupner@nttsecurity.com

Georg Graupner
arbeitet seit 2011 im Bereich IT, seit 2013 in IT-Sicherheitsprojekten. Als Senior IT Consultant von NTT Security ist er in der Kundenberatung tätig – vor allem im Bereich der Gestaltung von Sicherheitsmaßnahmen und Optimierung des Sicherheitsbetriebs für Applikationen. Seine fachlichen Schwerpunkte liegen in der Sicherheit von ERP-Systemen, der Anwendungsentwicklung sowie im Aufbau von IT-Security-Management-Lösungen nach gängigen Sicherheitsstandards. Außerdem hat er Erfahrungen im Bereich der Automotive Security, sowohl für Onboard- als auch für Offboard-Komponenten und -Prozesse.
Seinen Bachelor in Business Informatics hat er an der THI Ingolstadt um einen MBA in IT Management erweitert. Teile dieses Whitepapers stammen aus seiner Masterarbeit „Defense in Depth für Fahrzeuge – Stand der Technik und zukünftige Möglichkeiten“, publiziert im GRIN Verlag (www.grin.com/de).

11. Anhang

Impressum

NTT DATA Deutschland GmbH
Hans-Döllgast-Straße 26
80807 München
Deutschland
Telefon +49 89 9936 -0
de.nttdata.com

Bilder

Seite 1: Mopic / Shutterstock
Seite 2: Wutzkohphoto / Shutterstock
Seite 4: Chesky / Shutterstock
Seite 6/7: Metamorworks / Shutterstock
Seite 12: Chesky / Shutterstock
Seite 13: Sergey Nivens / Shutterstock
Seite 16: Sfio Cracho / Shutterstock

Danksagung

- René Bader, Manager for Critical Business Applications and Big Data bei NTT Security
- Jens Krüger, Competence Unit Manager und Leiter des globalen Center of Excellence für Product-Lifecycle-Management bei NTT DATA
- Odine Mansury, Manager Industrie Marketing Automotive & Manufacturing
- Niklas Bielmeier, Industrie Marketing Automotive & Manufacturing bei NTT DATA

Über NTT DATA

NTT DATA ist ein führender Anbieter von Business- und IT-Lösungen und globaler Innovationspartner seiner Kunden. Der japanische Konzern mit Hauptsitz in Tokio ist in über 50 Ländern weltweit vertreten.

Der Schwerpunkt liegt auf langfristigen Kundenbeziehungen: Dazu kombiniert NTT DATA globale Präsenz mit lokaler Marktkenntnis und bietet erstklassige, professionelle Dienstleistungen von der Beratung und Systementwicklung bis hin zum Outsourcing.

Weitere Informationen finden Sie auf de.nttdata.com

NTT DATA Deutschland GmbH
Hans-Döllgast-Straße 26
80807 München
Deutschland
Telefon +49 89 9936 -0
de.nttdata.com