Seminar IT-Sicherheit im Wintersemester 2017/18

IT Sicherheit bei Nutzfahrzeugen

Eingereicht am:

21. Januar 2018

Eingereicht von:

Tim Schott

wing100653@fh-wedel.de

Dozent:

Prof. Dr. Gerd Beuster

Fachhochschule Wedel

Feldstraße 143

22880 Wedel

gb@fh-wedel.de

Inhaltsverzeichnis: Seite

1. Einleitung

1.1. Wie war die Situation der IT-Sicherheit bisher?

In der Vergangenheit war es so, dass Nutzfahrzeuge sehr einfach gebaute Fahrzeuge waren, die lediglich ihre Primärfunktion erfüllten um Waren und Güter von A nach B zu transportieren. Da die ersten Nutzfahrzeuge am Ende des 19. Jahrhunderts entstanden, das Internet gegen 1970 entstand und erst 20 Jahre später kommerzialisiert wurde, gab es annähernd 100 Jahre lang keine Berührungspunkte zwischen Nutzfahrzeugen und dem Internet.

Dennoch gab es schon vorher mögliche Berührungspunkte der IT-Sicherheit mit dem Nutzfahrzeugbau. Ab 1982 gab es die ersten Funkfernbedienungen für die Zentralverriegelung. Schon zu diesem Zeitpunkt war es technisch möglich diese Verbindung zu stören und somit Nutzfahrzeuge zu entwenden. Ab diesem Zeitpunkt mussten sich Fahrzeugbauer über die IT-Sicherheit Gedanken machen.

In den letzten Jahren wurde dann immer mehr elektronisch/elektrisch gesteuert. Es gab eben nicht mehr nur die Zentralverriegelung sondern auch elektrische Fensterheber, Schiebedächer, Navigationssysteme und Kontrollsysteme für den Fahrer, die allesamt nach und nach auch ferngesteuert oder fernüberwacht werden konnten, was sie aber auch zu potentiellen Angriffszielen macht.

1.2. Wie wird die Situation in der Zukunft sein?

Die meisten Fahrzeughersteller gehen davon aus, dass die Schwerpunkte der Entwicklung zukünftig in den Bereichen, der Elektromobilität, dem autonomen Fahren und der Vernetzung von Fahrzeugen liegen [McK16]. Auf diese drei Bereiche wird sich der Schwerpunkt der Forschung in den nächsten 10 bis 15 Jahre fokussieren.

Für die drei Bereiche, Elektromobilität, autonomes Fahren und die Vernetzung, steigt die Menge an Funktionen die ein Fahrzeug hat. Neben der Anzahl, werden die Funktionen, die die Fahrzeuge bisher hatten, wesentlich anspruchsvoller. Aus diesen beiden Punkten resultiert, dass die Software die in jedem Fahrzeug steckt zunehmend umfangreicher wird. Durch die zunehmende Vernetzung, die Zunahme an Funktionen, die wachsende Komplexität, steigt auch der Anspruch an die IT-Sicherheit.

“Complexity is the worst enemy of security” [Sch12].

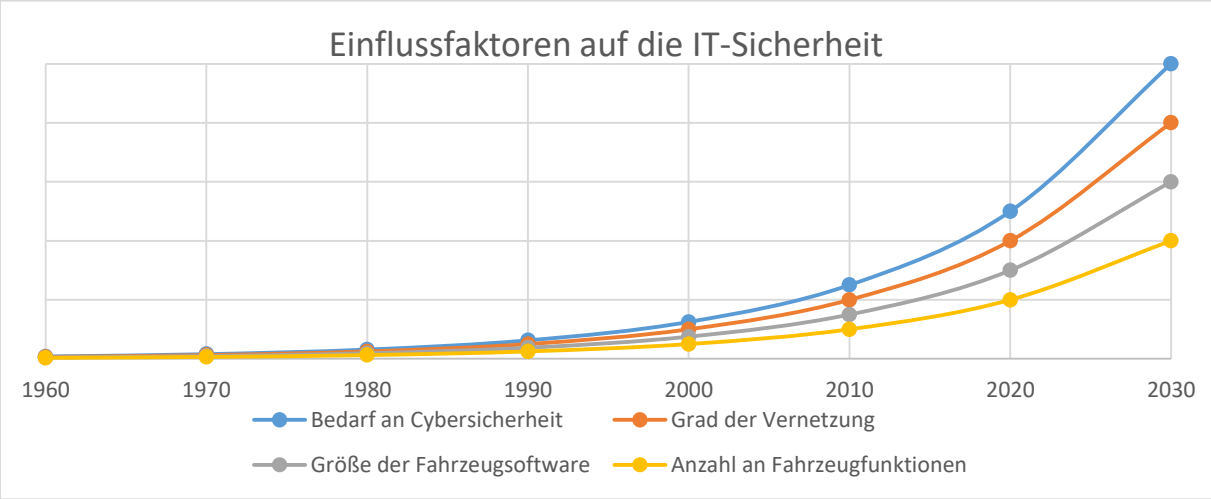

Bild 1: Einflussfaktoren auf die IT-Sicherheit [Cha09].

1.3. Warum sind Nutzfahrzeuge stärker von kriminellen Angriffen betroffen als Personenwagen?

Nutzfahrzeuge benutzen komplexere und umfangreichere von Software gesteuerte Funktionen. Ein gutes Beispiel ist das „Platooning“. Diese Vernetzung von Fahrzeugen ermöglicht es, dass viele Fahrzeuge dicht hintereinander fahren, der Sicherheitsabstand elektronisch auf ein Minimalmaß reduziert und somit der Windschatten optimal ausgenutzt wird. Hierdurch ist es möglich 3-5 % Kraftstoff zu sparen, die Sicherheit durch eine verringerte Staugefahr zu erhöhen, so wie die Fahrer zu entlasten, da die ganze Fahrzeugkolonne lediglich durch den Fahrer des Führungsfahrzeuges gesteuert wird. So werden beispielsweise Bremsvorgänge des Führungsfahrzeuges auf alle folgenden, vernetzten Fahrzeuge übertagen.

Ebenfalls wird es notwendig sein, dass bei Nutzfahrzeugen für ein professionelles Flottenmanagement mehr Daten entstehen, ausgetauscht und verarbeiten werden als bei Personenwagen. Die hierzu verwendeten Kommunikationswege senden über lange Distanzen, mit einem sehr starken Signal, wie beispielsweise mittels LTE (Long Term Evolution). In diesem Zusammenhang lässt sich auch noch sagen, dass Nutzfahrzeuge stärker standardisiert sind, bezüglich verbauter Teile und Protokollen und somit für Angreifer besser geeignet sind.

Auch ist der Wert eines Nutzfahrzeuges in der Regel wesentlich höher als der eines Personenwagens. Normalerweise kostet ein Nutzfahrzeug mehr als 100.000 €. Addiert man die transportierte Ware mit auf, so steigt der Wert eines Nutzfahrzeuges schnell, auf über 1.000.000 €. Ein weiterer beachtenswerter Aspekt besteht in dem Transportrisiko, durch transportierte Gefahrstoffe, von denen eine hohe Gefährdung für Mensch und Umwelt ausgeht. Zudem sind Nutzfahrzeuge durchschnittlich 20h pro Tag in Betrieb. Sie legen die 3-fache Strecke zurück, sind 5-mal so groß und 30-mal so schwer wie ein typischer Personenwagen.

Aus diesen Punkten ergibt sich, im Vergleich zu einem PKW, dass es einfacher ist einen Angriff/Diebstahl auf ein Nutzfahrzeug durchzuführen, da der Wert eines Nutzfahrzeuges oder die Anzahl an Daten die über ein Nutzfahrzeug erlangt werden können, höher sind und es einfacher ist einen Angriff/Diebstahl nahezu eins zu eins zu wiederholen.

2. Risiken der IT-Sicherheit

Auch wenn Nutzfahrzeuge von außen betrachtet doch beträchtlich von PKWs abweichen, so unterscheidet sich die E/E-Architektur (Elektrisch-/Elektronische Architektur) doch kaum. Die Nutzfahrzeuge bestehen wie in Bild 2 gezeigt aus nahezu 50 elektronischen Steuereinheiten, die untereinander über standardisierte Netzwerke kommunizieren wie beispielsweise CAN (Controller Area Network). Des Weiteren verfügen sie (Fahrer, Steuerelemente, einzelne Fahrzeugbaugruppen) über eine Anzahl differenzierter Möglichkeiten um mit der Außenwelt zu kommunizieren. So verfügen viele Nutzfahrzeuge über Wi-Fi und LTE.

Die daraus resultierenden Hauptrisiken sind, physischer Diebstahl, Manipulation der Fahrzeugfunktion/-Daten, Datendiebstahl oder Missbrauch sowie Angriffe auf die Fahrzeug Zuverlässigkeit und Sicherheit. Diese Risiken werden mittels folgender Tabelle bewertet, in der die Angriffserfolgswahrscheinlichkeiten den Schadenshöhen gegenübergestellt werden [SW12].

Angriffserfolgswahrscheinlichkeit↓	Sicherheitsrisikobewertung			
Hoch	Mittel	Hoch	Hoch	Hoch
Möglich	Klein	Mittel	Hoch	Hoch
Unwahrscheinlich	Unbedeutend	Klein	Mittel	Hoch
Sehr selten	Unbedeutend	Unbedeutend	Klein	Mittel
Schaden→	Vernachlässigbar	Signifikant	Kritisch	Katastrophe

Tabelle 1: Sicherheitsrisikobewertung [SW12]

2.1. Physischer Diebstahl

Physischer Diebstahl des ganzen Fahrzeuges oder wertvoller Fahrzeugteile ist die älteste und bekannteste Art eines Sicherheitsrisikos. In der folgenden Tabelle wird dieses Risiko aus dem Blickwinkel des PKW und des Nutzfahrzeuges verglichen. Der Risiko Fokus liegt auf dem Vergleich von: möglichen Diebstählen, typischen Dieben, Wahrscheinlichkeit eines Diebstahl, den Geschädigten und dem Schadenspotenzial.

Sicherheitsrisikobewertung physischer Diebstahl	PKW	Nutzfahrzeug
Mögliche Diebstähle	Airbags, Navigationssysteme, ganzes Fahrzeug	Navigationssysteme, Fahrzeug, Ladung, Anhänger oder Fahrzeug mit Anhänger und Ladung
Typische Angreifer	Organisiertes Verbrechen	Organisiertes Verbrechen
Wahrscheinlichkeit eines Diebstahls	Möglich	Möglich
Geschädigte	Besitzer	Besitzer, Fahrer und Kunde
Schadenpotenzial	Signifikant	Kritisch
Daraus resultierendes Risiko	**Mittel**	**Hoch**

Tabelle 2: Sicherheitsrisikobewertung pysischer Diebstahl [ASS17]

Um das Nutzfahrzeug zu stehlen, können die Diebe, die Sicherheitslücken der Keyless-Go Funktion nutzen. Die Keyless-Go Funktion von Nutzfahrzeugen unterscheidet sich kaum von denen in PKWs. Um ein Nutzfahrzeug zu stehlen muss lediglich das Signal der Keyless-Go Fernbedienung verlängert werden. Hierzu steht einer der Täter neben dem Fahrer und sendet das Signal mittels eines kleinen Gerätes an ein zweites, dieses befindet sich bei einem zweiten Täter der dann sein Gerät wie einen zweiten Schlüssel verwenden kann. Er kann das Fahrzeug öffnen und sogar starten und wenn er das Fahrzeug nicht abwürgt, geht das Fahrzeug auch nicht aus wenn der erste Täter nicht mehr das Signal der Keyless-Go Fernbedienung an ihn sendet.

Zusätzlich können über Wireless Schnittstellen, wie Wifi oder Bluetooth, „Öffnen“-Signale an das Fahrzeug übermittelt werden, da dies aber ein wesentlich größeres Know-how erfordert und mehr Zeit in Anspruch nimmt, greifen die meisten Diebe auf die Möglichkeit, die die Keyless-Go Funktion bietet, zurück.

2.2. Manipulation der Fahrzeugfunktionen/-daten

Zusammen mit den physischen Fahrzeugdiebstählen sind nicht autorisierte Manipulationen der Fahrzeugdaten und Funktionen die am meist verbreiteten Angriffe auf die IT-Sicherheit von Fahrzeugen. Normalerweise sind es Angriffe von innen, durch den Besitzer oder Fahrer des Fahrzeuges, oftmals durch

die Unterstützung von spezialisierten Firmen. Dies macht es sehr schwierig sich dagegen zu schützen. Der Angreifer hat für die Manipulation viel Zeit, da durch den Eigner/Fahrer keine Eigenanzeige und somit keine direkte Strafverfolgung droht.

Am häufigsten werden Funktionen manipuliert die dem Umweltschutz dienen, wie Beispielsweise die Abgasreinigung. Da die Reinigungsfunktionen mit einem erhöhten Kraftstoffverbrauch verbunden ist, ist durch eine entsprechende Modifikation dieser Funktion, kostenintensiver Kraftstoff einzusparen [Bo17]. Außerdem werden Funktionen zur Fahrsicherheit verändert, wie die Tachomanipulation, um schneller fahren zu können (LKWs werden elektronisch abgeregelt), hierdurch reduzieren sich die Fahrt- und Transportzeiten der Ware. Zudem kann, bei einem möglichen Weiterverkauf eines Nutzfahrzeuges der Kilometerzähler manipuliert werden, um den Verkaufswert zu steigern. Des Weitern gibt es Möglichkeiten bei dem Modell: „bezahlen durch benutzen“ zu manipulieren, sei es weil ein Fahrzeug nur eine festgelegt Kilometerzahl pro Jahr zurücklegen darf, wie beim Leasing beispielsweise [Law08].

Sicherheitsrisikobewertung Manipulationen der Fahrzeugfunktionen/-daten	PKW	Nutzfahrzeug
Mögliche Manipulationen	Chip-tuning, Kilometerstandmanipulation, umgehen von bezahlen durch Benutzen Funktion	Chip-tuning, Tachomanipulation, umgehen von Sicherheitsbestimmungen, umgehen von bezahlen durch Benutzen Funktion, manipulieren von Ladungsaufzeichnungen
Typischer Angreifer	Besitzer	Besitzer, Fahrer
Wahrscheinlichkeit der Manipulation	Unwahrscheinlich	Möglich
Geschädigter	Gesellschaft, eine dritte Person, Fahrzeugbauer	Gesellschaft, eine dritte Person, Fahrzeugbauer
Schadenspotential	Signifikant	Mindestens Signifikant
Daraus resultierendes Risiko	**Klein**	**Mittel**

Tabelle 3: Sicherheitsrisikobewertung Manipulation der Fahrzeugfunktionen/-daten [ASS17]

Bei der modernen E/E-Architektur sind häufig keine physischen Angriffe auf das Fahrzeug notwendig um Fahrzeugfunktionen oder –daten zu manipulieren. Der Angriff nutzt häufig einfach zugängliche Fahrzeugdiagnosesysteme, da diese ihm erlauben Zugriff auf alle elektronischen Steuerelemente zu nehmen. Um die Funktionen oder Daten zu manipulieren müssen dann lediglich einige versteckte Befehle mit den neuen Befehlen überschrieben werden. Bei Nutzfahrzeugen kann sich ein Angreifer das standardisierte Protokoll SAE J1939 (beschreibt die Kommunikation auf einem CAN-Bus in Nutzfahrzeugen zur Übermittlung von Diagnosedaten und Steuerungsinformationen) zunutze machen. Dieses kommt in fast allen LKWs zum Einsatz [BHM16].

Durch derartige Manipulationen, werden nicht bloß Leasingfirmen, gewerbliche Käufer von Gebrauchtfahrzeugen und private Käufer betrogen, sondern auch das Image von Kraftfahrzeug Herstellern geschädigt. Zusätzlich erhöht sich durch derartige Manipulationen das Unfall Risiko, wenn Nutzfahrzeuge die zulässige Höchstgeschwindigkeit (LKWs 80km/h, Busse 100km/h) überschreiten. Bezogen auf die Manipulation der Abgasreinigung, haben erhöhte Abgaswerte nicht nur einen schlechten Einfluss auf unsere Umwelt sondern auch auf die Gesundheit von uns allen

2.3. Datendiebstahl oder Missbrauch

Der Datendiebstahl und der Missbrauch dieser Daten hat sich inzwischen zu einem Milliarden Geschäft entwickelt. Der bekannteste Datendiebstahl ist der von IPs (IP=„Intellectual Property“ also geistiges Eigentum) um kostengünstiger und schneller, Konkurrenzprodukte oder Fälschungen zu produzieren. Der finanzielle Schaden durch Fälschungen beträgt in der gesamten Automobil-Industrie ca. 12 Milliarden US-Dollar. Besonders problematisch ist das Sicherheitsrisiko, welches durch solche gefälschten Produkte entsteht und keine Entwicklungsfirma die Produkthaftung übernimmt. Derartige IP-Diebstähle sind meistens Diebstähle von Insidern oder Experten, welche beispielsweise einen Chip ausbauen und die Daten darauf auslesen [Sko01].

Es gibt aber auch Datendiebstähle bei der die Privatsphäre verletzt wird. So werden unter anderem Daten aufgezeichnet, gespeichert und verändert welche die Fahrzeugposition, den Fahrzeugbetrieb und die Fahrer Kommunikation betreffen. Diese Daten werden genutzt um Gewährleistungsansprüche abzuweisen, individuelles Marketing zu betreiben, Daten an Dritte zu verkaufen oder um diese Daten, im Falle eines Unfalls, gegen den Fahrer zu verwenden.

Sicherheitsrisikobewertung Datendiebstahl oder Missbrauch	PKW	Nutzfahrzeug
Mögliche Datendiebstähle/-missbräuche	IP-Diebstahl, Verletzung der Privatsphäre, Fälschungen	IP- oder Geschäftsgeheimnis-Diebstahl, Verletzung der Privatsphäre, Fälschungen, Aufzeichnung der Routen, Ladungs- oder Navigation Manipulation, Fahrer Erpressung
Typische Angreifer	Produktfälscher, Konkurrenz, Versicherungen, Fahrzeugbauer	Produktfälscher, Konkurrenz, Versicherungen, Fahrzeugbauer, Regierungen, Organisiertes Verbrechen
Wahrscheinlichkeit Datendiebstahl/-missbrauch	Möglich	Möglich
Geschädigte	Fahrer, Besitzer, Fahrzeugbauer	Fahrer, Besitzer, Fahrzeugbauer, Kunde, Gesellschaft
Schadenspotential	Signifikant	Kritisch
Daraus resultierendes Risiko	**Mittel**	**Hoch**

Tabelle 4: Sicherheitsrisikobewertung Datendiebstahl oder Missbrauch [ASS17]

2.4. Angriffe auf die Fahrzeug Zuverlässigkeit und Sicherheit

Dank dem standardisierten Protokoll J1939, das in fast allen modernen Nutzfahrzeugen zum Einsatz kommt, ist es nicht notwendig, dass der Hacker mittels Reverse Engineering die internen Kommandos herausfinden muss [BHM16]. Dadurch entfällt der schwierigste und zeitintensivste schritt beim Hacken.

Bis jetzt gab es noch keinerlei solcher Angriffe auf Nutzfahrzeuge, da sie sehr aufwendig durchzuführen sind und sich keinerlei direkter finanzieller Nutzen daraus ergibt. Dennoch könnte diese Art des Angriffes von Terroristen genutzt werden, da ein 40 Tonnen schwerer und möglicherweise noch mit Gefahrgut beladener LKW schwersten Schaden anrichten kann.

Sicherheitsrisikobewertung Angriffe auf die Fahrzeug Zuverlässigkeit und Sicherheit	PKW	Nutzfahrzeug
Mögliche Angriffe	Löschen Kritischer Daten, Steuern/Sperren von Fahrzeugfunktionen (Bremsen)	Löschen Kritischer Daten, Steuern/Sperren von Fahrzeugfunktionen (Bremsen)
Typischer Angreifer	Erpresser, Terroristen	Erpresser, Terroristen
Wahrscheinlichkeit eines Angriffs	Sehr selten	Unwahrscheinlich
Geschädigter	Fahrer, Gesellschaft	Fahrer, Kunde, Gesellschaft
Schadenspotential	Katastrophe	Katastrophe
Daraus resultierendes Risiko	**Mittel**	**Hoch**

Tabelle 5: Sicherheitsrisikobewertung Angriffe auf die Fahrzeug Zuverlässigkeit und Sicherheit [ASS17]

3. Schutz vor Risiken der IT-Sicherheit

Im Folgenden wird das gesamtheitliche mehr Schichten Schutzsystem dargelegt. Mithilfe dieses Systems sollen die Risiken der IT-Sicherheit bei Nutzfahrzeugen reduziert werden. Das System deckt die folgenden drei Bereiche ab, Schutz des Gesamtsystems, Schutz über die gesamte Lebensdauer des Produkts, Schutz über alle Bereiche der Nutzfahrzeug Organisation. In den drei Bereichen wird die Umsetzung der Schutzmechanismen im Detail beschrieben und man wird sehen, dass einiges von den Schutzmechanismen aktuell schon bei den PKWs praktische Anwendung findet und in Teilen analog zu diesen PKW-Schutzmechanismen auf die Nutzfahrzeuge übertragen werden könnten.

3.1. Schutz des Gesamtsystems

Für den kompletten Fahrzeugschutz, muss das Fahrzeug von jeder einzelnen Steuereinheit bis hin zu allen mit dem Fahrzeug verbundenen Diensten betrachtet werden, da ein Angreifer immer nach dem einfachsten Zugang zum Fahrzeug suchen würde.

Um das Fahrzeug wirklich gut zu Schützen ist es wirkungsvoll, wenn man nicht nur einen Schutzmechanismus für einen Bereich verwendet, sondern jeden Bereich gleich mehrfach absichert. Dies ist deshalb wichtig, da einige Sicherheitsvorkehrungen mit der Zeit an Wirksamkeit verlieren oder aber auch einfach Versagen. Besonders, wenn zum Beispiel eine einzelne Firewall das interne Fahrzeugnetzwerk schützen würde. Wäre diese Firewall „geknackt“, dann könnte es sein, dass es durch die flächendeckende Standardisierung möglich wäre, alle Nutzfahrzeuge auf der Welt zu „knacken“.

In der folgenden Grafik ist ein mögliches Sicherheitsnetzwerk für ein Fahrzeug Schematisch dargestellt. Dieses Sicherheitsnetzwerk besteht aus mehreren Schichten, jede Schicht besteht aus einem anderen Sicherheitsmechanismus. Anzunehmen ist, dass hierbei nicht alle Sicherheitssysteme auf einmal versagen und somit ein hoher Sicherheitsstandard erreicht wird.

3.2. Schutz über die Gesamte Lebensdauer des Produkts

Im Gegensatz zum klassischen Fahrzeugbau, wo die Aufgaben des Fahrzeugbauers eigentlich abgeschlossen sind, sobald das Fahrzeug das Werk verlassen hat, ist es bei der IT Sicherheit notwendig die Sicherheit solange sicherzustellen bis das Fahrzeug tatsächlich nicht mehr benutzt wird. Dieser Prozess kann bei Nutzfahrzeugen 10 in seltenen Fällen sogar 20 Jahre und länger dauern. Besonders bei der IT-Sicherheit ist, dass sich das zu Schützende ständig wandelt und die Angreifer immer neue Wege und Mittel suchen, um sich Zugriff zu verschaffen. Auch ist es möglich, dass neue und bessere Sicherheitsvorkehrungen entwickelt werden, die dann natürlich auch bei Fahrzeugen genutzt werden sollten die bereits auf der Straße fahren.

Hierfür gibt es einen „IT-Sicherheitskreislauf des Lebens“ [ASS17]. Dieser soll dafür sorgen, dass über die gesamte Produktlebensdauer die IT-Sicherheit gewährleistet ist.

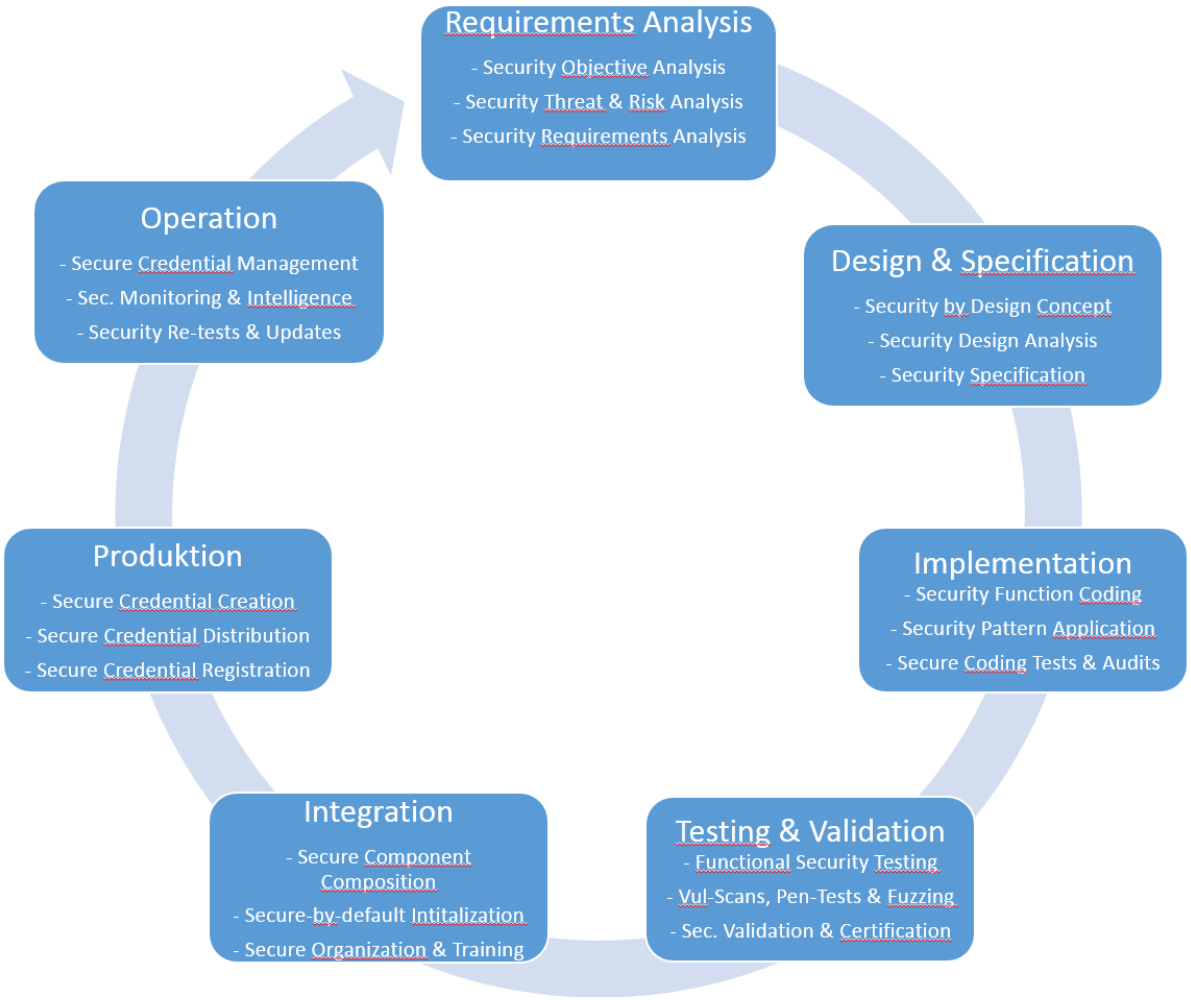

Bild 4: IT-Sicherheitskreislauf des Lebens [ASS17]

3.3. Schutz über alle Bereiche der Nutzfahrzeug Organisation

Die IT-Sicherheit bei Nutzfahrzeugen, ist heutzutage eine Abteilungsübergreifende Aufgabenstellung. Besonders da durch die IT-Sicherheit weder neue Anwendungen noch zusätzliche Umsätze generiert werden.

Wichtig ist alle Abteilungen mit einzubeziehen, da sich die IT-Sicherheit auf alle Fahrzeugkomponenten bezieht und diese alle in einem Fahrzeug zusammen, sicher und geschützt, arbeiten sollen. Diese Sicherheit endet aber nicht mehr beim Fahrzeug sondern erstreckt sich auch auf alle Dienste, Steuerelemente und Anwender die mit diesem Fahrzeug verbunden sind. Auch kann es sinnvoll sein manche Sicherheitsmechanismen an anderen Stellen im Fahrzeug ebenfalls anzuwenden. Entwickelte Algorithmen können in einem Unternehmen bei weiteren Sicherheitsmechanismen zur Anwendung kommen. Es können somit an unterschiedlichen Stellen Synergieeffekte genutzt werden.

Im Folgenden werden die wichtigsten Rollen, einer unabhängigen Sicherheitsarchitektur der Nutzfahrzeugorganisation, beschrieben.

Vehicle Security Officer (VSO):

Dies ist eine zusätzliche Rolle eines Team Mitgliedes. Diese Person ist Teil von allen anderen Bereichen, wie Entwicklung, Testing, Produktion, Operation und abteilungsübergreifenden Divisionen, wie dem Qualitätsmanagement. Der VSO sorgt dafür, dass alle Teammitglieder Schulungen im Bereich der IT-Sicherheit bekommen, die Regeln und Prozesse der IT-Sicherheit angewendet werden. Er bewirbt neue Sicherheitsverfahren und berichtet über neue Risiken der IT-Sicherheit und die neuen Sicherheits-Voraussetzungen, Möglichkeiten und Verbesserungen der Fahrzeugsicherheit.

Vehicle Security Center (VSC):

Ist ein Team von IT-Sicherheitsexperten im Bereich von Nutzfahrzeugen. Diese sorgen für die Entwicklung und Pflege der IT-Sicherheits-Prozedur und –Richtlinien. Das VSC arbeitet eng mit dem VSIRT (Vehicle Security Incident and Response Team) zusammen um Sicherheitsrisiken zu bewerten und wenn nötig entsprechende Gegenmaßnahmen zu koordinieren. Auch arbeitet das VSC mit vielen anderen Firmenbereichen zusammen, wie beispielsweise der Rechtsabteilung um alle Richtlinien immer auf dem aktuellen Stand zu halten. Des Weiteren ist das VSC für interne IT-Sicherheitsschulungen verantwortlich. Geführt wird das VSC vom Chief Vehicle Security Officer.

Vehicle Security Incident and Response Team (VSIRT):

Ist ein Team aus IT-Sicherheitsexperten, das sich auf neue IT-Sicherheitsrisiken um alle Firmenprodukte fokussiert. Das VSIRT überblickt die Medien, IT-Sicherheitskonferenzen und -Komitees, spricht mit Kunden und Mitarbeitern und hat sogar die Mitbewerber im Blick. Manchmal werden sogar sogenannte „white hacker“ hinzugezogen. Das VSIRT ist zusätzlich für die Ausführung und das Anfragen von Analysen zur IT-Sicherheit da.

Chief Vehicle Security Officer:

Sitzt der IT-Sicherheit vor. Der CVSO entscheidet über die Strategie und führt die gesamte IT-Sicherheit. Bei kritischen Entscheidungen ist er für diese verantwortlich. Der CVSO berichtet direkt an die Geschäftsführung und kann somit auch im gesamten Unternehmen Entscheidungen herbeiführen.

4. Zusammenfassung und Ausblick

In dieser Arbeit wurden die Risiken der IT-Sicherheit von Nutzfahrzeugen beschrieben, die die Sicherheit, Zuverlässigkeit und die Geschäftstätigkeit entsprechender Fahrzeuge beeinflussen. Diese Risiken wurden mit denen von Personenwagen verglichen. Aus diesen identifizierten Risiken wurde dann ein Schutzsystem entwickelt mit dem ein gesamtheitlicher Schutz eines Nutzfahrzeuges über die gesamte Lebensdauer eines Fahrzeuges in allen Bereichen sichergestellt werden kann.

Die Analyse hat gezeigt das Nutzfahrzeuge durch ein oftmals viel höheres Angriffsrisiko von IT-Gefahren betroffen sind als Personenwagen. Da beim Nutzfahrzeug häufig mehr Parteien geschädigt werden, der Schaden größer ist, die Angriffsziele vielfältiger sind und ein Angriff leichter durchzuführen ist.

Auch wurde gezeigt, dass viele Schutzfunktionen die in Personenwagen schon Anwendung finden analog auch bei Nutzfahrzeugen eingesetzt werden können. Für die Zukunft denke ich müssen die Nutzfahrzeughersteller sicherstellen, ein Schutzsystem wie das oben beschriebene zu entwickeln und in den praktischen Einsatz zu bringen, damit die Sicherheit bei den Herausforderungen der Zukunft, wie der Elektro Mobilität, dem autonomen Fahren und der Vernetzung von Kraftfahrzeugen gewährleitet werden kann.

5. Literaturverzeichnis

[ASS17] Marko Wolf und Robert Lambert, “Hacking Trucks – Cybersecurity Risks and Effective Cybersecurity Protection for Heavy Duty Vehicles“, in GI Edition Automotive – Safety & Security 2017, 2017, Ausgabe 269, S. 45-60.

[BHM16] Yelizaveta Burakova et al., “Truck Hacking: An Experimental Analysis of the SAE J1939 Standard”, in WOOT’16 Protokoll des 10. USENIX Workshop on Offensive Technologies, 2016, S. 211-220.

[Bo17] Christian Bock (2017): “Die Lüge vom sauberen LKW”, <https://www.zdf.de/dokumentation/zdfzoom/zdfzoom-die-luege-vom-sauberen-lkw-100.html>, in ZDF Zoom < https://www.zdf.de/dokumentation/zdfzoom/>, Revisionsdatum: 21.01.2018.

[Cha09] Robert Charette (2009): “This car runs on code”, <https://spectrum.ieee.org/transportation/systems/this-car-runs-on-code>, in IEEE Spectrum <https://spectrum.ieee.org>, Revisionsdatum: 21.01.2018.

[Law08] Nate Lawson (2008): “Highway to Hell: Hacking Toll Systems”, <https://media.blackhat.com/bh-usa-08/video/bh-us-08-Lawson/black-hat-usa-08-lawson-hackingtollsystems-hires.m4v>, in Blackhat USA 2008 <http://www.blackhat.com/html/bh-usa-08/bh-usa-08-archive.html>, Revisionsdatum: 21.01.2018

[McK16] McKinsey (2016), “Automotive Revolution Perspective Towards 2030”, <https://www.mckinsey.de/files/automotive_revolution_perspective_towards_2030.pdf>, in Advanced Industries < https://www.mckinsey.de/advanced-industries>, Revisionsdatum: 21.01.2018

[Sch12] Bruce Schneier (2012): „Complexity the Worst Enemy of Security“, https://www.schneier.com/news/archives/2012/12/complexity_the_worst.html, in Schneier Security Blog <https://www.schneier.com>, Revisionsdatum: 21.01.2018

[Sko01] Sergei P. Skorobogatov (2001): “Copy Protection in Modern Microcontrollers”, <http://www.cl.cam.ac.uk/~sps32/mcu_lock.html>, in University of Cambridge – Department of Computer Science <http://www.cl.cam.ac.uk>, Revisionsdatum: 21.01.2018

[SW12] Michael Scheibel et al. (2012): “A Systematic Approach to a Quantified Security Risk Analysis for Vehicular IT Systems", <http://www.marko-wolf.de/files/WoSc12_Automotive_SRA.pdf in Automotive Safety & Security, November 2012>, in Automotive Safety & Security, Revisionsdatum: 21.01.2018