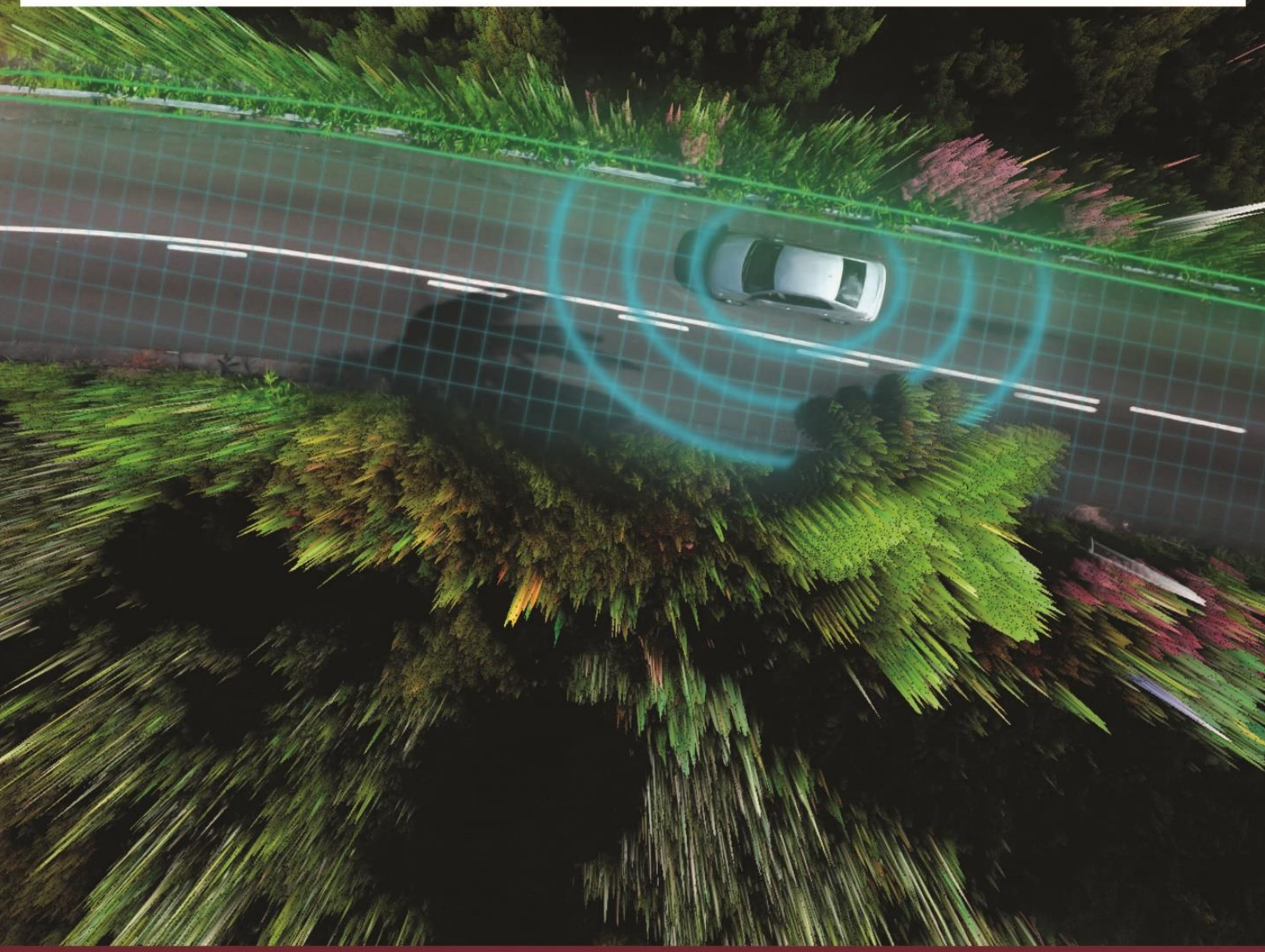
Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•



Branchenlagebild Automotive

Cyber-Sicherheit in der Automobilbranche

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582- 0
E-Mail: bsi@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Einleitung

Die Automobilbranche ist ein Industriezweig, der sich in erster Linie der Massenproduktion von Automobilen und anderen Kraftfahrzeugen widmet. Hierzu zählen neben den Automobilherstellern auch deren Zulieferer, Entwickler und sonstigen Dienstleister. Es ist somit die größte Branche des verarbeitenden Gewerbes und gemessen am Umsatz der mit Abstand bedeutendste Industriezweig in Deutschland.

Cyber-Angriffe werden qualitativ immer ausgereifter und zielgerichteter. Insbesondere Ransomware-Angriffe sind aus Sicht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) aktuell die größte operative Bedrohung der Cyber-Sicherheit. Als Einfallstor nutzen die Angreifer in der Regel die Office-IT-Netzwerke und stellen hohe Lösegeldforderungen, unter der Androhung, sensible Daten bei Nichtzahlung zu veröffentlichen. Gleichzeitig wird die Abhängigkeit und Vernetzung der IT-Infrastrukturen von Automobilherstellern und deren Zulieferern (Supply-Chain) immer größer, wodurch sich die potentielle Angriffsfläche weiter erhöht und das Schadenspotenzial zunimmt.

Die COVID-19-Pandemie hat gezeigt, welche Bedeutung funktionierende und sichere IT-Infrastrukturen haben. Cyber-Sicherheit muss deshalb bei allen Digitalisierungsvorhaben einen Schwerpunkt bilden und von Anfang an mitgedacht und umgesetzt werden. Dies gilt insbesondere vor dem Hintergrund, dass Automotive alle Aktivitäten im Bereich von Zulieferteilen, -produkten oder -dienstleistungen der Automobilbranche abbildet.

Das BSI gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft, als Voraussetzung einer erfolgreichen Digitalisierung. Für mehr Sicherheit neuer Technologien, wie z.B. Künstliche Intelligenz, 5G oder Smart Home/Smart Factory, gestaltet das BSI u. a. praxisgerechte Sicherheitsanforderungen, Standards und Handlungsempfehlungen. Das BSI unterstützt beispielsweise bei der Absicherung einer digitalisierten Verkehrsinfrastruktur, als Basis für autonomes Fahren.

Dieser Bericht liefert hierzu einen branchenspezifischen Überblick zur Lage der Cyber-Sicherheit im Bereich „Automotive“, sowohl hinsichtlich der Produktion als auch der Fahrzeuge selbst. Er macht deutlich, wie wichtig diese Aufgabe ist und dass die Herausforderungen vielfältig und komplex sind.

2 Managementübersicht zur Gesamtlage

Die Digitalisierung hat in modernen Autos und Verkehrsinfrastrukturen sowie in den Unternehmen der Automobilbranche längst Einzug gehalten. Technologien wie die Fahrzeug-zu-Fahrzeug-Kommunikation und 5G sollen das Autofahren sicherer und komfortabler machen. Durch die Digitalisierung werden neue Dienstleistungen und Funktionen im Fahrzeug ermöglicht. In dem Maße, in dem Fahrzeuge mit der Außenwelt vernetzt sind, nimmt auch die Angriffsfläche und damit die Bedeutung von Cyber-Sicherheit in der Automobilbranche zu.

Damit mögliche Cyber-Angriffe keinen Einfluss auf die Fahrsicherheit haben und geeignete Schutzmechanismen integriert werden können, müssen entsprechende Gefährdungen bereits frühzeitig im Entwicklungszyklus neuer Fahrzeugmodelle berücksichtigt werden. Moderne Autos sind längst fahrende Hochleistungsrechner und in erheblichem Maße von digitaler Technik gesteuert. Wenn digitale Technologien genutzt werden sollen, um Autos vernetzt und automatisiert fahren zu lassen, sowie die Verkehrssicherheit zu erhöhen, dürfen diese Technologien nicht durch unbefugte Dritte manipulierbar sein.

Ransomware-Angriffe sind aus Sicht des BSI aktuell die größte operative Bedrohung der Cyber-Sicherheit. Sie haben aufgrund der ausgeprägten Schadwirkung und der verstärkten Androhung einer Veröffentlichung zuvor gestohlener Daten ein neues Gefahrenpotential für die Betroffenen erreicht. Auch international zeigt sich die zunehmende Betroffenheit. So setzt die aktuelle US-Regierung das Thema Cyber-Sicherheit weit nach oben auf die Tagesordnung, nachdem eine Reihe von öffentlichkeitswirksamen Angriffen mit weitreichenden, kollateralen Auswirkungen auf andere Bereiche, den USA weit mehr geschadet haben, als den einzelnen betroffenen Unternehmen.

Die erste und wichtigste Motivation der Angreifer für die Verbreitung von Ransomware ist der finanzielle Gewinn. Insbesondere große Unternehmen, welche aus monetärer Sicht potentiell höchst lohnenswerte Ziele darstellen, werden immer wieder Opfer solcher Angriffe (Big Game Hunting). Im Bereich der Automobilbranche erfolgen Angriffe insbesondere auf die Supply Chain und die stark vernetzten Infrastrukturen der Office-IT und der Produktionsanlagen, nicht auf die IT der Fahrzeuge. Beispiele zeigen, dass solche Angriffe unabhängig von Branchen oder Nationen erfolgen. Automobilhersteller und ihre Zulieferer (Supply-Chain-Angriffe), aber auch kleinere Betriebe mit Alleinstellungsmerkmalen, wie zum Beispiel die Produktion spezieller Komponenten im Maschinenbau, wurden in jüngster Vergangenheit Opfer von gezielten Cyber-Angriffen:

- In 2017 kam es bei einem französischen Automobilhersteller zu einem Stillstand der kompletten Produktion, ausgelöst durch die Schadsoftware „WannaCry“. Auch dessen Zulieferer waren durch die Auswirkungen betroffen und konnten keine Teile liefern.
- 2020 wurden die Systeme eines deutschen Zulieferers und Dienstleisters verschlüsselt. Mehrere Gigabyte Daten mit Konstruktionszeichnungen und Arbeitsplänen sind abgeflossen.
- Ebenfalls in 2020 kam es bei einem amerikanischen Zulieferer in Folge eines Ransomware-Angriffs zu massiven Produktionseinschränkungen und zu Lieferproblemen.
- 2021 waren mehrere deutsche Zulieferer und Entwickler Opfer von Ransomware-Angriffen. In Folge kam es zu massiven Unterbrechungen deren Leistungserbringung.

Um den für den Wirtschafts- und Automobilstandort Deutschland wichtigen Bereich der Digitalisierung sicher zu gestalten und verlässliche Rahmenbedingungen für Investitionen und Innovationen zu schaffen, arbeiten das BSI und das Kraftfahrt-Bundesamt (KBA) zukünftig in Fragen der Cyber-Sicherheit eng zusammen. Mit neuen Regeln für die Genehmigung von Fahrzeugen sollen beispielsweise das Thema Cyber-Sicherheit in der Fahrzeugentwicklung fest verankert und Risiken besser vorgebeugt werden. Der für den Transfer in die Anwendung erforderliche Austausch mit der Automobilindustrie wird dabei proaktiv durch das BSI und den Verband der deutschen Automobilindustrie (VDA) vorangetrieben.

3 Cyber-Sicherheit in der Automobilbranche

Die Automobilbranche ist durch nationale, wie auch internationale Vorgaben stark reguliert. Im Bereich der Typgenehmigung[1] sind für Deutschland und die Mitgliedsstaaten der Europäischen Union die Vorgaben von entsprechenden EU-Verordnungen maßgeblich. Diese verweisen hinsichtlich der technischen Anhänge häufig auf Regelungen der Wirtschaftskommission für Europa der Vereinten Nationen (UNECE), welche für etwa sechzig weitere Vertragsstaaten maßgeblich sind[2].

In über 150 Einzelregelungen werden technische Vorgaben und Prüfverfahren vor allen Dingen zur Verkehrssicherheit des Fahrzeugs definiert. Seit kurzem werden hier auch explizit Anforderungen an die Cyber-Sicherheit gestellt. Innerhalb der EU wird eine durch einen Mitgliedsstaat einmal erteilte Typgenehmigung auch in anderen Mitgliedstaaten anerkannt.

Innerhalb Deutschlands ist die Industrie im Verband der deutschen Automobilindustrie (VDA) organisiert. Auf europäischer Ebene wird die Branche durch die Association des Constructeurs Européens d'Automobiles (ACEA) und die European Association of Automotive Suppliers (CLEPA) repräsentiert.

3.1 Branchenüberblick

Die Branche setzt sich aus den Automobilherstellern, deren Zulieferern, Entwicklern und sonstigen Dienstleistern zusammen. Es handelt sich um die größte Branche des verarbeitenden Gewerbes und den Industriezweig mit dem größten Umsatz in Deutschland.

2020 wurde nach vorläufigen Zahlen ein Gesamtumsatz von etwa 378 Mrd. Euro (davon 135 Mrd. Euro im Inland) erzielt. Es waren im Jahresdurchschnitt etwa 809.000 Personen in dieser Industrie beschäftigt. In Deutschland wurden 2020 ca. 3.500.000 Fahrzeuge (ohne Nutzfahrzeuge) produziert. Im Jahr 2018 haben die weltweiten Aufwendungen deutscher Unternehmen der Branche für Forschung und Entwicklung 44,6 Mrd. Euro betragen (1).

3.2 Gefahren durch Cybercrime

Cyberkriminelle Angriffe werden hinsichtlich ihrer Schadenswirkung in den vergangenen Jahren von Ransomware-Angriffen dominiert. Hierbei geht insbesondere von sogenannten Big Game Hunting (zu Deutsch Großwildjagd) Ransomware-Angriffen ein herausragendes Bedrohungspotenzial aus. Diese Angriffe richten sich gegen besonders solvente Organisationen, betreffen zumeist große Teile des Opfernetzwerks und sind opportunistisch. Durch diese opportunistische Vorgehensweise sind derartige Angriffe eine Bedrohung für jede Art von Organisation und Unternehmen und somit auch für die Automobilbranche.

Durch die teilweise eng miteinander verzahnten Supply-Chains (Lieferketten) in der Automobilbranche ergibt sich für einen Betroffenen darüber hinaus ein hoher Handlungsdruck, das operative Geschäft nach einem Vorfall schnell wiederherzustellen. Dieser Druck kann von einem cyberkriminellen Angreifer für die Lösegeldverhandlung ausgenutzt werden.

Verschiedene Cybercrime-Gruppierungen leiten vor der Verschlüsselung sensible Daten aus, beispielsweise Informationen über Prototypen. Diese werden dann auszugsweise veröffentlicht, um den Druck auf das Opfer zu erhöhen. Üblicherweise erfolgt eine Bekanntgabe des Opfers auf der jeweiligen Webseite der Täter mit dem Hinweis, wie viele und welche Daten abgeflossen sind. Die erste und wichtigste Motivation für die

[1] Mit der Typgenehmigung wird bestätigt, dass ein serienmäßig in größerer Stückzahl hergestellter Typ gleichartiger Fahrzeuge oder Fahrzeugteile den gesetzlichen Vorschriften entspricht. In Deutschland ist hierfür das Kraftfahrt-Bundesamt (KBA) zuständig.

[2] Auf Grundlage des Genfer Übereinkommen vom 20. März 1958

Verbreitung von Ransomware ist der finanzielle Gewinn. Forderungen die erfüllt werden, ermuntern einen Täter bei ähnlich gelagerten folgenden Fällen eine höhere Forderung zu stellen.

Angriffe mit Ransomware haben aufgrund der ausgeprägten Schadwirkung und der verstärkten Androhung einer Veröffentlichung zuvor gestohlener Daten ein neues Gefahrenpotential für die Betroffenen erreicht. Einige davon sorgten wegen des z. T. länger anhaltenden Ausfalls der jeweiligen kritischen Dienstleistung national und international für besonderes Aufsehen (siehe Kapitel *Managementübersicht zur Gesamtlage*).

Ransomware ist für Cyber-Kriminelle ein seit Jahren etabliertes Geschäftsmodell und betrifft Desktop-Betriebssysteme wie Microsoft Windows und Apple Mac OS, sowie Server-Systeme unter Windows und Linux. Infektionsvektoren von Ransomware sind aktuell E-Mail-Anhänge oder Spam-Mails mit verlinkter Schadsoftware, sowie Schwachstellen in aus dem Internet erreichbaren Server-Systemen.

Die folgenden Punkte zeigen, warum sich das Geschäftsmodell für die Angreifer rentiert:

- Hoher Leidensdruck auf Seiten der Opfer.
- Bei Geschädigten sind i. d. R. die Verluste oder die Wiederherstellungsaufwände größer als die Erpressersumme.
- Zahlungen in Bitcoins oder Monero sind anonym und sofort realisierbar. Sie müssen nicht aufwändig über Geldboten/Moneymules und Warenagenten getätigt werden.

Insbesondere bei Ransomware-Vorfällen treten Versäumnisse bei der Prävention häufig deutlich zutage. Schlecht gepflegte Systeme, fehlende, veraltete oder nicht überprüfte Software-Backups, schwache Administrator-Passworte, fehlende Netzsegmentierung u.v.a.m. „rächen“ sich bei Ransomware sofort durch die eingetretenen Schäden. Auch das Verhalten der Mitarbeiter spielt eine zentrale Rolle. Einige Angriffe werden mittlerweile durch Nutzung legitimer Namen und E-Mails so täuschend echt, dass sie nur schwer zu erkennen sind. Andere der beobachteten Ransomware-Kampagnen (Spamwellen) sind hingegen nicht mit großem Aufwand gestaltet. Hier würde eine bessere Sensibilisierung der Mitarbeiter helfen.

3.3 Qualifizierung von Schlüsselpersonal im Bereich Informations- und Cyber-Sicherheit

Mitarbeiter in der Produktion sind selten in Cyber-Sicherheit geschult und erwarten keine gezielte Manipulation. Es gibt in diesem Bereich selten Arbeitsanweisungen, wie bei Verdacht auf Anlagenmanipulation umgegangen werden soll. Zudem ist es nicht ohne weiteres möglich, aus einem ungewöhnlichen Verhalten der Produktionsanlage auf einen Angriff zu schließen. Mentale Vorbereitung, Awareness und Übungen mit Einbeziehung der Produktion, werden unter dem Gesichtspunkt der Cyber-Sicherheit bisher eher selten durchgeführt.

Durch die Größe der Automobilbranche sowie dem Wachstum in Innovationsbereichen ist der Bedarf an ausreichend qualifiziertem Personal nur schwer zu decken. Hinzu kommt, dass gerade bei kleineren Zulieferern und Dienstleistern sowie Startups oftmals das Risiko, Opfer eines Cyber-Angriffes zu werden, unterschätzt wird.

3.4 Bedeutung der Informationssicherheit in der Supply Chain

Die gesamte Automobilbranche ist geprägt von einer hohen Arbeitsteilung. Die Automobilhersteller sind eng mit den Zulieferern verzahnt. Dazu werden unter anderem sensible Informationen wie beispielsweise Konstruktionsdaten geteilt. Zudem können Beeinträchtigungen in der Fertigung bei Zulieferern schnell Auswirkungen auf die Automobilhersteller haben.

Ein Beispiel ist der Angriff auf einen deutschen Hersteller von Karosserieteilen Anfang 2021, bei dem Konstruktionsdaten und Arbeitspläne der Kunden gestohlen und veröffentlicht wurden.

Ein weiteres Beispiel stellt der Angriff im Jahr 2020 auf einen amerikanischen Zulieferer dar, bei dem ebenfalls sensible Informationen gestohlen wurden.

Nicht nur der Diebstahl solcher Informationen stellt ein Problem dar. Insbesondere Produktionseinschränkungen können zu einem Problem führen. Die vielen Beispiele von Ransomware-Angriffen auf Unternehmen zeigen, dass eine Produktionsunterbrechung von einer Woche oder sogar mehr verursacht wird, selbst wenn die Produktionsanlagen nicht direkt von dem Ransomware-Angriff betroffen sind. Hieraus können sich wie in einer Kettenreaktion Auswirkungen entlang der Supply Chain ergeben.

Auch Dienstleister für Wartung und Service bei Produktionsanlagen stellen ein mögliches Einfallstor dar. Dies zeigt der Fall eines weltweit agierenden Dienstleistungsunternehmens im Juli 2021. Hierbei nutzten die Angreifer mehrere Schwachstellen in einer Software aus, die von zahlreichen Service Providern zur Wartung von Kundennetzen eingesetzt wird. Die Angreifer konnten so über den Service Provider deren Kunden angreifen und Systeme kompromittieren.

3.5 Auswirkung der „neuen Normalität“ auf die Informations- und Cyber-Sicherheit

Spätestens seit den Auswirkungen der COVID-19-Pandemie verlegen viele Organisationen Büroarbeitsplätze zunehmend ins Home-Office, um ihren Betrieb zumindest eingeschränkt aufrechterhalten zu können, so auch in der Automobilbranche. Diese tiefgreifende Veränderung bringt jedoch zahlreiche Herausforderungen mit sich, da IT-Infrastrukturen signifikant angepasst werden müssen, insbesondere bei der erstmaligen Einrichtung von Heimarbeitsplätzen sowie Remote-Zugriffen.

Der Umgang mit dienstlichen Unterlagen oder Informationen mit erhöhtem Schutzbedarf am Heimarbeitsplatz sollte durch erweiterte, hochwertige technische Sicherungsmaßnahmen geschützt werden. Es werden vermehrt Phishing Kampagnen beobachtet, die aktuelle Krisen-Situationen ausnutzen und versuchen, sensible Daten abzugreifen, mit Schlagwörtern wie „Remote-Zugänge“ oder das angeblich erforderliche „Zurücksetzen von Passwörtern“. Am Heimarbeitsplatz können Angreifer häufig einfacher auf vertrauliche Informationen zugreifen. Werden Informationen unberechtigt gelesen oder preisgegeben, hat dies schwerwiegende Folgen für das gesamte Unternehmen. Unter anderem kann es zu Wettbewerbsnachteilen oder finanziellen Schäden kommen.

Zumeist ist der Heimarbeitsplatz nicht so gut abgesichert wie der Arbeitsplatz in einem Unternehmen. Ist das Home-Office bzw. das mobile Arbeiten in einem Unternehmen nicht oder nur unzureichend geregelt, entstehen verschiedene Sicherheitsrisiken. Der oben genannte Abfluss von Informationen stellt dabei nur eines von zahlreichen Bedrohungsszenarien dar. Dies kann auch insbesondere bei der vermehrten Nutzung von Web-Konferenz-Systemen geschehen, beispielsweise durch das versehentliche Freigeben einer Bildschirmpräsentation. Daher muss für alle Heimarbeitsplätze geregelt sein, wer welche Informationen außerhalb der Institution weitergeben und verarbeiten darf und welche Schutzvorkehrungen (Sicherheitsmaßnahmen) dabei umzusetzen sind (2).

4 Cyber-Sicherheit im Fahrzeug sowie in digitalen Produkten

Im Zuge der globalen Technologietrends in der Automobilbranche (Konnektivität, Automatisierung, Sharing, Elektrifizierung) nimmt die Cyber-Sicherheit in Fahrzeugen insbesondere in Bezug auf die Vernetzung der zugrundeliegenden IT-Infrastrukturen der Automatisierung eine Schlüsselrolle ein. Durch die zunehmende Vernetzung ergeben sich vielfältige denkbare Angriffswege mit hohem Schadenspotential, was die Einbeziehung der IT-Sicherheit in der Produktentwicklung unumgänglich macht.

4.1 Vernetztes Fahren

Während Fahrzeuge in der Vergangenheit als abgeschlossene Systeme konzipiert wurden, verfügen moderne Fahrzeuge über eine Vielzahl an drahtlosen Kommunikations-Schnittstellen (Connected Mobility). In vielen Modellen sind Telematikeinheiten verbaut, die über LTE oder 5G mit dem Internet und gegebenenfalls mit einem Hersteller-Backend verbunden sind. Ebenso werden in vielen Infotainmentsystemen ähnliche Technologien wie in modernen Smartphones eingesetzt. Dies beinhaltet neben der Konnektivität auch vergleichbare Betriebssysteme und Apps.

Die Vernetzung eröffnet neue Möglichkeiten, Fahrzeug-Daten mit dem Hersteller, aber auch Dritten zu teilen. Die notwendigen Zugriffskonzepte (3) (4) dafür werden umfassend diskutiert, wobei zwei mögliche Zugriffsmethoden im Fokus stehen. Der Zugriff ausschließlich über das Hersteller-Backend, oder direkt über eine sich im Fahrzeug befindliche Plattform.

In C-ITS (Cooperative Intelligent Transport Systems) kommunizieren Fahrzeuge mit anderen Fahrzeugen sowie mit der Verkehrsinfrastruktur (z. B. Ampel-Systemen), was die Verkehrssicherheit erhöhen soll. Über signierte C-ITS Nachrichten kann zum Beispiel vor Verkehr aus schlecht einsehbaren Straßen gewarnt oder über die Länge von Ampelphasen informiert werden.

Eine Vernetzung kann ebenfalls über nachträglich eingebaute OBD2-Dongles[3] erfolgen. Diese Geräte, die an die OBD2-Schnittstelle des Fahrzeugs angeschlossen werden, können etwa zu Fahrzeugdiagnosezwecken eingesetzt werden und leiten dazu Daten aus dem internen Fahrzeugnetzwerk an Mobilgeräte weiter. Versicherungen und Flottenbetreiber können mit OBD2-Dongles Informationen zum Fahrverhalten abrufen.

Ein weiterer Aspekt der (lokalen) Vernetzung ergibt sich aus der E-Mobilität. Die Ladeschnittstelle von E- und Hybridfahrzeugen ist weit komplexer als eine einfache Steckdose. Über standardisierte Protokolle müssen Informationen zwischen Ladeeinrichtung und dem Lademanagement des Fahrzeugs ausgetauscht werden, um einen sicheren Ladevorgang zu ermöglichen. Zukünftig sollen auch Zahlungsinformationen direkt über die Ladeinfrastruktur übermittelt werden, was eine geeignete Sicherheitsinfrastruktur im Hintergrund erfordert.

4.2 Automatisierung und Künstliche Intelligenz

Der massive Einsatz von Sensorik, Rechenleistung und KI-Algorithmen verspricht, dass Autos „intelligenter“ werden und langfristig sogar komplett autonom agieren können (Automated Mobility). Zur Erreichung höherer Autonomiestufen in Fahrzeugen ist der Einsatz von Künstlicher Intelligenz (KI), auch für sicherheitskritische Funktionen, in vielen Fällen unumgänglich. Die stetig steigende Qualität und Quantität von Daten, als auch die steigende Rechenleistung, haben zu enormen Fortschritten in der Performanz von KI-Systemen geführt, sodass diese bereits jetzt verschiedenste Funktionalitäten umsetzen können. In diesem Kontext sind beispielsweise die Detektion und Klassifikation von Verkehrsschildern oder Automatisierungs- und Assistenz-Funktionen zu nennen. Gleichzeitig bietet der Einsatz von KI-Systemen

[3] On-Board-Diagnose

neue Angriffsmöglichkeiten. Angreifer können gezielt versuchen, Sensoreingabedaten zu manipulieren (z. B. durch unauffällige Aufkleber auf Verkehrsschildern), um ein gewünschtes Fehlverhalten des Fahrzeugs auszulösen. Auch in der Trainingsphase der Lernalgorithmen könnten Angreifer versuchen, manipulierte Daten einzubringen, die später zu Fehlfunktionen führen (5).

Nach und nach halten automatisierte Fahrfunktionen auch in handelsüblichen Kraftfahrzeugen Einzug. Die ersten Systeme fallen in den Medien allerdings immer wieder durch Unfälle auf, die teils mit der nicht ausreichenden Marktreife, aber vor allem auch mit dem Fehlverhalten der Nutzer zusammenhängen. Während sich in der Vergangenheit verschiedene Automatisierungsfunktionen unter Laborbedingungen aus der Ferne manipulieren ließen, ist bisher kein Fall bekannt, bei dem ein Fahrer im Straßenverkehr Opfer eines solchen aktiven Angriffes wurde.

4.3 Angriffsmöglichkeiten auf digitale Produkte

In jüngster Vergangenheit haben zahlreiche Studien aufgezeigt, dass es mit gewissem Aufwand durchaus möglich ist, zentrale Komponenten im Fahrzeug anzugreifen bzw. über Schwachstellen einen unbefugten Zugriff auf sensible Funktionalitäten der Fahrzeugsicherheit zu erlangen und diese zu manipulieren. Hierzu einige Beispiele:

- Im Mai 2021 veröffentlichte ein Sicherheitsforscher einen Bericht zu Schwachstellen in Infotainmentsystemen bestimmter Fahrzeuge. Durch Schwachstellen des integrierten Browsers und des veralteten Linux-Betriebssystems, ließen sich verschiedene Infotainmentfunktionen, wie die Innenbeleuchtung und das Display, durch einen Fernzugriff manipulieren. Ebenso konnten über eine kompromittierte Debug-Version einer Komponente beliebige Nachrichten auf den CAN-Bus[4] geschickt werden. Der Hersteller wurde über die Schwachstellen informiert und hat diese umgehend durch einen Softwarepatch beseitigt.
- Im April 2021 veröffentlichte ein Sicherheitsforscher einen Bericht, welcher zwei Schwachstellen in der Open-Source-Software „ConnMan“ beschreibt, über die ein Angreifer in das Center Information Display (CID) eindringen kann. Durch einen Stack-Buffer-Overflow bei der Verarbeitung von DNS-Antworten können so auf dem CID im Fahrzeug Code ausgeführt werden. Der Zugang selbst wird über einen W-LAN Hotspot hergestellt, mit dem sich parkende Fahrzeuge automatisch verbinden und dessen Anmeldedaten schon länger öffentlich bekannt sind. Auf diesem Wege ließe sich das Display beeinflussen oder, wie von den Forschern demonstriert, das Auto aus der Ferne (innerhalb des W-LAN Bereiches) öffnen.
- 2020 wurde in einer Analyse (6) gezeigt, dass eine große Anzahl von OBD-Dongles auf vielfältige Weise angegriffen werden kann. Während bei einem Teil der 77 getesteten Modelle nur Fahrzeugdaten auszulesen waren, konnte in manchen Fällen das Fahrzeug geöffnet, oder auf den zentralen CAN-Bus zugegriffen werden, um beispielsweise das Fahrverhalten zu beeinflussen.

[4] Controller Area Network

5 Cyber-Sicherheit in Produktionsanlagen und -prozessen

Der Grad der Vernetzung und Automatisierung wird insbesondere im Bereich der Produktion deutlich. In modernen Fertigungsstraßen sind nahezu alle Komponenten, von Sensoren bis hin zu Fertigungsrobotern, untereinander verbunden. Hierdurch erhöht sich auch die Angriffsfläche, da diese Systeme auch an das Unternehmensnetzwerk und Dienstleister-Netzwerke angeschlossen sein können und teilweise auch über das Internet erreichbar sein sollen.

5.1 Digitalisierung in der Produktion

Die Digitalisierung in der Produktion schreitet immer weiter voran. Ein guter Indikator dafür ist die Anzahl der in der Produktion genutzten IP-Adressen, die sich bei manchen Automobilherstellern zeitweilig exponentiell entwickelt hat, während sie im Office-Bereich eher konstant blieb oder sich sogar verringerte. Mit der steigenden Digitalisierung (z. B. Industrie 4.0, Nutzung von Cloud) in der Produktion sinkt die Resilienz. Ein Inselbetrieb, der eine Weiterführung der Produktion bei Ausfall der Office-Systeme erlauben würde, ist immer seltener möglich. Vor allem die immer weiter fortschreitenden Individualisierungsmöglichkeiten machen einen Austausch zwischen den Ebenen erforderlich. Damit einhergehend steigen zum einen Abhängigkeiten zwischen diesen Ebenen und zum anderen Gefahren für eine Ausbreitung von Schadsoftware. Die Abhängigkeiten zeigen sich bei einem Ausfall oder der Beeinträchtigung von Diensten des Unternehmensnetzes. Ein erfolgreicher Angriff auf das Unternehmensnetzwerk hat schnell Auswirkungen auf die Produktion.

In der Produktion kommen nur selten Angriffserkennungssysteme, insbesondere zur Logdatenauswertung oder Anomalieerkennung, zum Einsatz. Sollte ein Angreifer persistenten Zugang in eine Produktionsumgebung erlangen, so stehen die Chancen hoch, dass er lange nicht entdeckt wird. Aktuell ist es jedoch einfacher, klassische IT-Systeme im Office-Bereich zu kompromittieren, um Schaden zu verursachen. Es gibt sowohl auf nationaler als auch internationaler Ebene Beispiele für Cyber-Angriffe, bei denen sich die Schadsoftware aus dem kompromittierten Unternehmensnetz in das Produktionsnetzwerk ausgebreitet hat, mit fatalen Folgen.

Im Falle von kriminellen, monetär motivierten Angreifern, ist zur Erhöhung des Drucks auf den Betreiber eine gezielte Manipulation und Kompromittierung der OT (Operational Technology)[5] in naher bis mittlerer Zukunft gut denkbar. Die entsprechenden Vorkehrungen wurden im Programmcode von Ransomware bereits 2020 gefunden. Die Umsetzung von „Best Practices“, einer strikten Trennung von Produktion und Office-Bereich, wie beispielsweise in der IEC 62443 beschrieben, wird durch die Abhängigkeiten und den notwendigen Austausch von Informationen erschwert. Genauer betrachtet haben sich die Bedrohungen in den letzten Jahren kaum verändert. In den BSI „TOP 10 Bedrohungen und Gegenmaßnamen für ICS“ (7) ändern sich lediglich die Trends hinsichtlich der Ausnutzbarkeit und deren Folgen. Die Bedrohungen selbst unterliegen nur geringen Änderungen.

Des Weiteren nimmt die Nutzung von sog. Commercial of the Shelf Produkten im industriellen Bereich zu, die auf Standardkomponenten und -betriebssystemen beruhen. Damit steigt die Angriffsfläche, weil Schwachstellen, welche zuvor nur aus der Office-IT bekannt waren, nun auch in der Produktion ausgenutzt werden können. Zwar hat auch der Einsatz von Backup-Strategien in der OT zugenommen, allerdings werden die notwendigen Wiederherstellungsprozeduren dafür nur selten in großem Maßstab getestet.

Eine weitere Herausforderung bei der Digitalisierung stellen die unterschiedlichen Verantwortungsbereiche hinsichtlich der klassischen IT und der Produktionsanlagen dar. Die spezifischen Anforderungen an die Funktionen (z. B. deterministische Echtzeitanforderungen der Steuerungen) und die geltenden gesetzlichen

[5] Operational Technology - Hard- und Software zur Steuerung und Überwachung physischer Maschinen und industrieller Anlagen

Regelungen (z. B. zum Schutz von Menschen vor Schäden durch Maschinen) erschweren die Zusammenarbeit. In den letzten Jahren ist zu beobachten, dass ein Wissenstransfer stattfindet und ein gegenseitiges Verständnis entsteht, um die Cyber-Sicherheit in der Produktion sicherzustellen. Die historische Trennung der Verantwortlichkeiten, verbunden mit unterschiedlichen Prioritäten und geringem Austausch des Personals untereinander, wird jedoch nur langsam abgebaut.

5.2 Umgang mit Schwachstellen

Der Umgang mit Schwachstellen, insbesondere der Soft- und Hardware von Produktionsanlagen, ist eine komplexe Herausforderung. Dabei bestehen zwei Hauptprobleme, die nicht allein für die Automobilbranche gelten. Auf der einen Seite etabliert sich die Versorgung mit Sicherheitsupdates bei vielen Herstellern erst langsam. Auf der anderen Seite werden für ältere Komponenten zum Teil gar keine Sicherheitsupdates bereitgestellt, so dass identifizierte Schwachstellen nicht geschlossen werden können und eine mögliche Ausnutzung anderweitig verhindert werden muss.

Die eingesetzten oft proprietären Kommunikationsprotokolle der Hersteller erfüllen aktuelle Sicherheitsanforderungen an Manipulationsschutz oft nicht. Aus Kompatibilitätsgründen werden diese früher seriellen Protokolle in IP verpackt und über Jahrzehnte weiterverwendet. Zudem treten in den eingesetzten Softwarelösungen oft komplexe Abhängigkeiten von externen Bibliotheken und Komponenten auf, die aktuell auch seitens der Hersteller und Integratoren nur unzureichend überwacht werden. Fehler in der Entwicklungsumgebung von Software wirken sich auf sehr viele Hersteller und noch mehr Produkte aus. Insbesondere im Netzwerkstack von Embedded-Systemen[6], dessen Code oft mehr als 10 Jahre alt ist, werden aktuell sehr viele Schachstellen bekannt.

Das Vorhandensein von zum Teil sehr alten Schwachstellen in Produktionsanlagen basiert oftmals auf einer Kombination aus unzureichendem Assetmanagement der eingesetzten Komponenten, über knappe Zeitfenster für das Einspielen von Sicherheitsupdates, sowie dem Problem, dass Informationen über Patches und Updates herstellerseitig meist nicht in einem standardisierten, maschinenlesbaren Format bereitgestellt werden. Das BSI treibt daher die Entwicklung des standardisierten Austauschformats CSAF (Common Security Advisory Framework) voran, welches in Kombination mit der Software Bill of Materials (SBOM) diesen Prozess unterstützen soll.

5.3 Dienstleister und Fernservices

Neben den Beziehungen mit Zulieferern für die Produktion von Fahrzeugen gibt es zahlreiche Verbindungen zu anderen Dienstleistern. Es kann sich dabei unter anderem um Dienstleistungen zur Überwachung, Wartung und Service für Produktionssysteme handeln. Diese werden vor dem Hintergrund von vorausschauender Wartung (Predictive-Maintenance) oder auch Pay-per-Use-Szenarien für Maschinen noch an Bedeutung gewinnen. Weitere Beispiele sind klassische Cloud-Anwendungen.

Bei Fernservices durch Dienstleister stellt sich wiederkehrend die Frage nach deren Vertrauenswürdigkeit. Grundsätzliches Problem dabei ist, den unberechtigten Zugriff auf Daten bei bzw. durch den Dienstleister zu verhindern. Es gilt zu regeln und sicherzustellen, wie die Verarbeitung von Daten erfolgen muss, um einen Missbrauch zu vermeiden. Gerade bei Fernzugriffen von Dienstleistern gilt es, unberechtigte Zugriffe oder, aufgrund der zunehmenden Vernetzung der IT-Infrastrukturen, die Ausbreitung von Ransomware zu verhindern. Hierzu sind entsprechende Nachweise zur Vertrauenswürdigkeit der Dienstleister und der Verarbeitung der Informationen notwendig. Eine Möglichkeit für Nachweise stellt der C5-Standard[7] des BSI (8) für Cloud-Anbieter dar. Dieser wurde auch bereits für KI-Anwendungen erweitert. Trotzdem bleibt die Gefahr, dass diese Zugänge missbraucht werden. Dies hat der o. g. Angriff auf ein weltweit agierendes Dienstleistungsunternehmen im Juli 2021 verdeutlicht.

[6] Embedded-Systeme bestehen i. d. R. aus Hardware, Software und Firmware. Sie sind „eingebettet“ in ein größeres System, um eine bestimmte Funktion zu erfüllen.

[7] Cloud Computing Compliance Criteria Catalogue (C5)

6 Maßnahmen und Aktivitäten

Um den für den Wirtschafts- und Automobilstandort Deutschland wichtigen Bereich der Digitalisierung sicher zu gestalten und verlässliche Rahmenbedingungen für Investitionen und Innovationen zu schaffen, arbeiten das BSI und das Kraftfahrt-Bundesamt (KBA) zukünftig in Fragen der Cyber-Sicherheit eng zusammen. Mit neuen Regeln für die Genehmigung von Fahrzeugen sollen beispielsweise das Thema Cyber-Sicherheit in der Fahrzeugentwicklung fest verankert und Risiken besser vorgebeugt werden. Der für den Transfer in die Anwendung erforderliche Austausch mit der Automobilindustrie wird dabei proaktiv durch das BSI und den Verband der deutschen Automobilindustrie (VDA) vorangetrieben.

6.1 Informationssicherheit im Unternehmen

Geschäftsabläufe hängen maßgeblich von Informationen und Informationssystemen und deren sicherer Verarbeitung ab. Informationssicherheit ist dabei mehr als nur eine Absicherung der technischen Infrastruktur – es bedeutet Sicherheit des gesamten Informationsflusses im Kontext der Vernetzung und Globalisierung.

Die Digitalisierung von Geschäftsprozessen über Unternehmensgrenzen hinweg erfordert daher ein vergleichbares Informationssicherheitsniveau aller Beteiligten, das über die gesamte Wertschöpfungskette gewährleistet wird, um geeignete Schutzmaßnahmen etablieren zu können.

Experten der Automobilbranche arbeiten dazu im VDA im Arbeitskreis Informationssicherheit zusammen, um gemeinsame Standards und angemessene Schutzmaßnahmen zu erarbeiten. Ein wesentliches Ergebnis der Zusammenarbeit ist ein Branchenstandard für Informationssicherheits-Assessments, der VDA Information Security Assessment (ISA) Katalog. Der Katalog ist Grundlage für das Branchenmodell TISAX[8], über das eine unternehmensübergreifende Anerkennung von Assessment-Ergebnissen gewährleistet wird. Mehr als 2.800 Unternehmen der Automobilbranche haben sich seit 2017 für TISAX registriert (9).

Die meisten deutschen Autohersteller fordern TISAX bereits in wichtigen Teilen ihrer Wertschöpfungskette. Es ist davon auszugehen, dass weitere Autohersteller sich dem anschließen werden.

6.2 Regulierung und Standardisierung - Vorgaben zur Cyber-Sicherheit

Die Anforderungen an die Typgenehmigung von Kraftfahrzeugen sind auf internationaler Ebene durch EU-Verordnungen harmonisiert. Diese verweisen in den zu erfüllenden Einzelvorgaben häufig auf UNECE Regelungen. Maßgeblich sind dabei die von der Wirtschaftskommission der Vereinten Nationen für Europa (United Nations Economic Commission for Europe, UNECE) erarbeiteten Vorgaben (10). Diese Vorgaben werden regelmäßig in europäisches Recht übernommen und somit auch in Deutschland wirksam. Die meisten dieser Vorgaben zielen auf die funktionale Sicherheit von Fahrzeugen ab. Für die neuen technologischen Entwicklungen hinsichtlich der Automatisierung und Vernetzung wurden zahlreiche neue Regelungen entwickelt, die 2020 von der UNECE beschlossen wurden und aktuell von den ersten Automobilherstellern umgesetzt werden.

Beispielsweise beinhaltet die UNECE R155 (11) neue Vorgaben zur Cyber-Sicherheit. Darin enthalten sind Prüfvorschriften für ein für die Automobilhersteller verpflichtendes Cybersecurity Management System (CSMS), das alle Phasen der Fahrzeugentwicklung umfassen soll. Mit betrachtet wird dabei auch die Nachsorge im Falle von neu auftretenden Schwachstellen oder Vorfällen (Incident Management). Das CSMS muss durch die zuständige nationale Behörde genehmigt werden. Für neue Fahrzeugtypen müssen Hersteller eine Risikobewertung nachweisen. Die technische Umsetzung der Maßnahmen zur Cyber-Sicherheit wird durch technische Dienste im Rahmen des Genehmigungsprozesses überprüft. Ergänzend dazu formuliert die neue Regulierung UNECE R156 (12) Anforderungen an Software Update Management

[8] Trusted Information Security Assessment Exchange

Systeme (SUMS) und die damit verbundenen Prozesse. Risiken, die sich durch die Möglichkeit von Software-Updates in Fahrzeugen ergeben, sind explizit zu betrachten. In der EU werden diese Regelungen ab Juli 2022 für neue Fahrzeugtypen mit einer Übergangsfrist bis Juli 2024 verpflichtend.

Im Mai 2021 wurde das Gesetz zum autonomen Fahren von Bundestag und Bundesrat beschlossen. Das Gesetz[9] legt u. a. fest, welche technischen Voraussetzungen für einen sicheren Betrieb zu gewährleisten sind, wie ein Fahrzeug im Bedarfsfall zu stoppen ist und dass es eine Möglichkeit geben muss, alternative Fahrmanöver aus der Ferne initiieren zu können. Zudem müssen die Fahrzeughersteller nachweisen, dass die elektronische Architektur des Fahrzeugs vor Cyber-Angriffen und Manipulationen geschützt ist.

Außerhalb der verpflichtenden Vorgaben arbeitet die Industrie an der ISO/SAE 21434 „Road Vehicles-Cybersecurity Engineering". In diesem Standard sollen Richtlinien für die Entwicklung und die Produktion von cyber-sicheren Fahrzeugen in Übereinstimmung mit den Anforderungen der UNECE R155 beschrieben werden.

6.3 Zusammenarbeit und Aktivitäten des BSI

Im Oktober 2020 haben das BSI und das KBA eine Verwaltungsvereinbarung zur Zusammenarbeit im Bereich der Cyber-Sicherheit von Kraftfahrzeugen geschlossen. Das BSI unterstützt das KBA bei den Prozessen zur Typgenehmigung nach den oben genannten neuen UNECE-Regelungen, ebenso wie bei IT-Sicherheitsfragen in der Marktüberwachung. Die ersten Verfahren zur Zertifizierung der CSMS und SUMS bei den Herstellern nach UNECE R155 und R156 werden derzeit vom BSI begleitet.

Im Juni 2020 unterzeichneten das BSI und der Verband der deutschen Automobilindustrie (VDA) eine Absichtserklärung, in der ein regelmäßiger Austausch zu Themen der IT-Sicherheit vereinbart wurde. Ziel ist es, ein gemeinsames Verständnis der verschiedenen Teilbereiche der Cyber-Sicherheit im Automobilbereich zu entwickeln, Handlungsbedarfe z. B. in der Standardisierung zu benennen und das Thema IT-Sicherheit in der Lieferkette aufzuarbeiten. Zudem sollen zukünftig weitere Workshops veranstaltet werden, die sich mit der sich stets weiterentwickelnden Cyber-Sicherheits-Landschaft für Fahrzeuge, Produkte und Lieferketten auseinandersetzen. Aus dieser Arbeit heraus sollen in der Folge Handlungsempfehlungen für die Politik und die Automobilbranche formuliert werden.

2021 wird das BSI zwei technische Richtlinien (TR-03164-1 und -2) zur IT-Sicherheit in C-ITS veröffentlichen. Die TR-03164-1 stellt eine Guidance für den Betrieb der PKI[10]-Instanzen in kooperativen intelligenten Verkehrssystemen auf Grundlage der einschlägigen ETSI[11]-Spezifikationen und der Certificate Policy der EU-Kommission dar. In der TR-03164-2 werden Empfehlungen für den sicheren Betrieb von C-ITS-Stationen, also den Hardware-Komponenten für die Fahrzeug-zu-X-Kommunikation und Road-Side-Units, formuliert.

Derzeit entwickelt das BSI im Rahmen eines Projektes zu Hard- und Softwareanalysen einen Leitfaden für Penetrationstests für vernetzte Fahrzeuge, der von Behörden, Prüfstellen und Unternehmen genutzt werden kann. Es sollen darin u. a. organisatorische und technische Voraussetzungen für die Durchführung der Penetrationstests beschrieben und die typischen drahtlosen und drahtgebundenen Schnittstellen eines vernetzten Fahrzeuges abgedeckt werden. Der Leitfaden wird voraussichtlich Ende des kommenden Jahres fertiggestellt.

[9] §1e f. Straßenverkehrsgesetz (StVG)
[10] Public Key Infrastruktur
[11] European Telecommunications Standards Institute

7 Chancen und Risiken: Ein Blick in die nahe Zukunft

Für die Branche und die Gesellschaft bietet sich durch die fortschreitende Digitalisierung von Fahrzeugen eine Vielzahl von Möglichkeiten zur Steigerung der Sicherheit und Effizienz im Straßenverkehr. Die Vernetzung ermöglicht neue Geschäftsmodelle, wie den Abruf von fahrzeuginternen Daten durch den Hersteller, aber auch durch Dritte wie zum Beispiel Flottenbetreiber, Werkstätten und Versicherer.

Es ist zu erwarten, dass in naher Zukunft weitere digitale Dienste im Fahrzeug angeboten werden, aus denen sich ein mehr oder weniger komplexes System aus Plattformen und Anwendungen entwickeln wird. Daraus ergeben sich Herausforderungen für die Cyber-Sicherheit des Gesamtprodukts Fahrzeug. Damit zusammenhängend ist das Problem der (Software-)Lieferkette im Automobilbereich zu betrachten. Komplexe Lieferketten bieten viele Einfallstore für manipulierte oder unzureichend geprüfte Hard- und Software und erschweren die Entwicklung von Updates im Fall von auftretenden Schwachstellen. Geeignete organisatorische Maßnahmen sind daher nötig, um diesen Risiken frühzeitig zu begegnen.

Die Möglichkeit, Updates per Funk einzuspielen, erlaubt es, Sicherheitslücken auch ohne einen Werkstatt-Rückruf zu beheben. Mit einer Neuregelung der Typgenehmigungsvorschriften wird erreicht, dass solche Updates genehmigungskonform eingespielt werden können.

Mit den neuen Technologien ergeben sich jedoch auch neue Risiken. Die neuen Funk-Schnittstellen im Fahrzeug, vor allem in Verbindung mit dem Infotainmentsystem, haben sich immer wieder als angreifbar herausgestellt. In extremen Fällen wird es einem Angreifer ermöglicht ein Auto fernzusteuern und somit den Fahrer direkt zu gefährden (13). Das Ziel von nationalen und internationalen Regulierungen und Standardisierungen sowie die einhergehenden Anforderungen an die Automobilhersteller ist es, dass derartige Schwachstellen bereits im Vorfeld erkannt oder zumindest zügig behoben werden können.

Mit Hilfe der Fahrzeug-zu-Fahrzeug- und Fahrzeug-zu-Infrastrukturkommunikation (C-ITS) sollen kritische Verkehrssituationen entschärft oder vermieden werden, um einen besseren Verkehrsfluss zu ermöglichen. Voraussetzung dafür ist ein breiter Einsatz dieser Technologien sowohl auf Fahrzeug- als auch auf Verkehrsinfrastrukturseite (wie z. B. Ampeln oder Baustellenwarner).

Im Zuge der Vernetzung und Automatisierung müssen auch Fragen des Datenschutzes sorgfältig betrachtet werden. Es muss eine datenschutzkonforme Nutzung der Dienste möglich sein und etwa ein Orts-Tracking von Verkehrsteilnehmern durch Dritte mit Hilfe von C-ITS-Nachrichten oder unerkanntes Aufzeichnen mit Hilfe von für das automatisierte Fahren notwendige Kameras vermieden werden.

Außerhalb des Fahrzeugs bieten auch Entwicklungen aus der Industrie 4.0 eine Chance für die Automobilbranche. Der Einsatz neuer Technologien und Vernetzungen können (theoretisch) genutzt werden, um die Produktion entlang der gesamten Lieferkette zu optimieren.

Die neuen Regelungen der UNECE R155 stellen einen Meilenstein für die Etablierung der Cyber-Sicherheit im Automobilbereich dar. Es bleibt nun zu beobachten, wie sich dieses Regelwerk in der Praxis bewähren wird. Aus den Diskussionen unter den Beteiligten ist bereits klar, dass die Vorgaben einen Interpretationsspielraum zulassen, so dass eine weitere Konkretisierung z. B. im Hinblick auf die Testumfänge wünschenswert erscheint.

Während die Möglichkeit, Updates einzuspielen, viele Vorteile für die Automobilhersteller hat, sind einige Rahmenbedingungen noch ungeklärt. So bleibt offen, wie lange Hersteller Updates zur Verfügung stellen müssen, was nach Ablauf dieser Zeiträume passiert und wer das finanzielle und materielle Risiko hierfür übernimmt.

Das Thema Cyber-Sicherheit wurde bereits frühzeitig von der Automobilbranche priorisiert. Durch die ganzheitliche Etablierung von nationalen und internationalen Regulierungen einerseits und durch die Schaffung eigener Standards (u. a. TISAX) andererseits, hat die Branche gute Voraussetzungen, angemessen auf eine sich verändernde Bedrohungslage (z. B. durch Big Game Hunting) zu reagieren und eine erfolgreiche Digitalisierung umzusetzen.

Literaturverzeichnis

1. **BMWI.** *Automobilindustrie.* https://www.bmwi.de : s.n., August 2021.

2. **BSI.** *Tipps für sicheres mobiles Arbeiten.* April 2021.

3. **VDA.** *Zugang zum Fahrzeug und zu im Fahrzeug generierten Daten.* 2016.

4. **FIA.** *On-Board Telematics Platform Security.* Juni 2020.

5. **von Twickel, A., Neu, M. Berghoff, C.** *Intelligente autonome Fahrzeuge, aber sicher.* s.l. : BSI-Magazin 2020/02, 2020.

6. **Haohuang Wen, Qi Alfred Chen, Zhiqiang Lin.** *Plug-N-Pwned: Comprehensive Vulnerability Analysis of OBD-II Dongles as a New Over-the-Air Attack Surface in Automotive IoT.* 2020.

7. **BSI.** *Industrial Control System Security - Top 10 Bedrohungen und Gegenmaßnahmen.* 2019.

8. **BSI**. *Cloud Computing Compliance Criteria Catalogue – C5.* 2020.

9. **VDA.** *Jahresbericht 2020.*

10. **UNECE.** *Agreement concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts [...] (Revision 3).* Oktober 2017.

11. **UNECE**. *E/ECE/TRANS/505/Rev.3/Add.154 - UN Regulation No. 155 - Cyber security and cyber security management system.* März 2021.

12. **UNECE**. *E/ECE/TRANS/505/Rev.3/Add.155 - UN Regulation No. 156 - Software update and software update management system.* März 2021.

13. **Charlie Miller, Chris Valasek.** *Remote Explotation of an Unaltered Passanger Vehicle.* 2015.