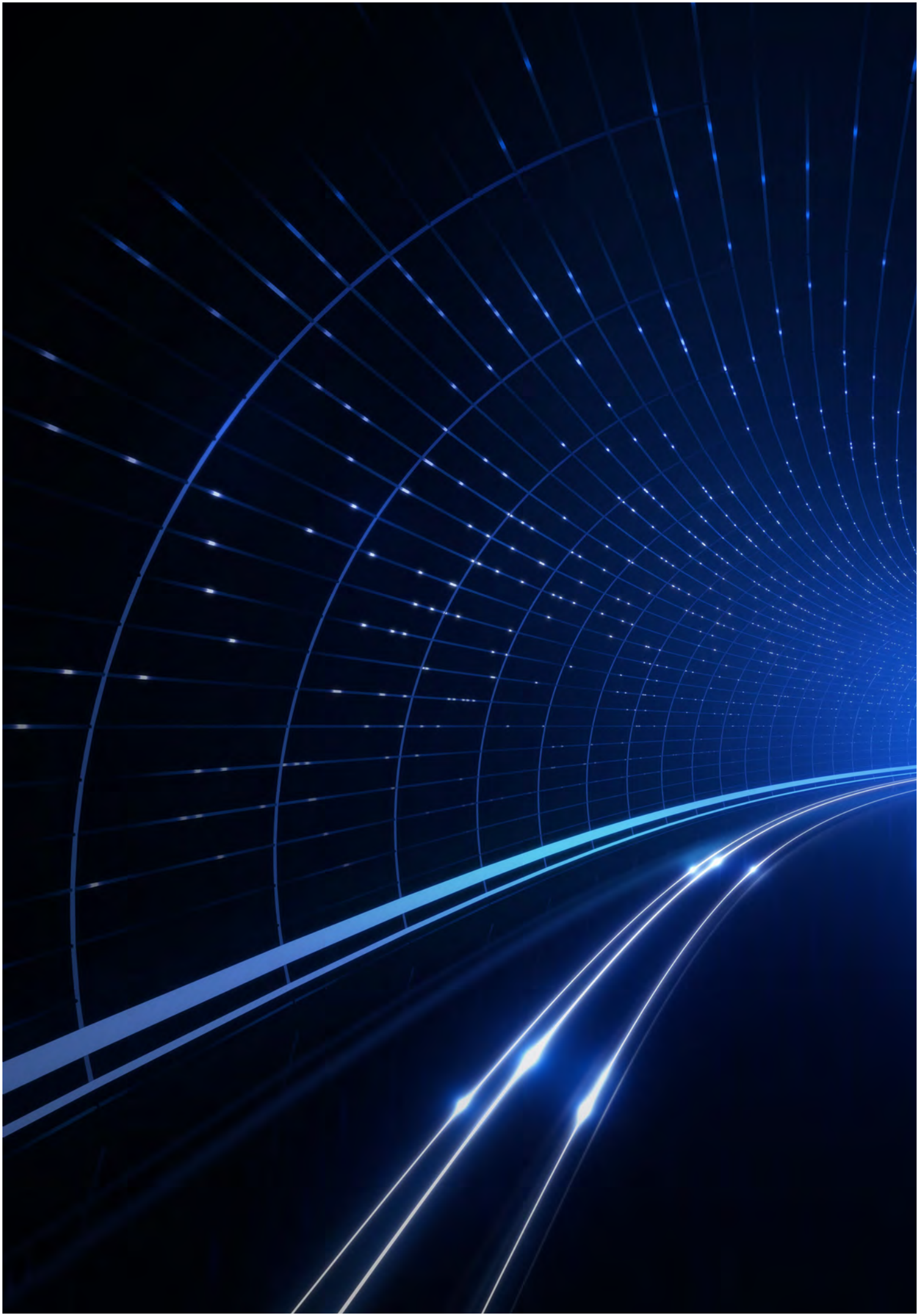
Branchen-lagebild Automotive

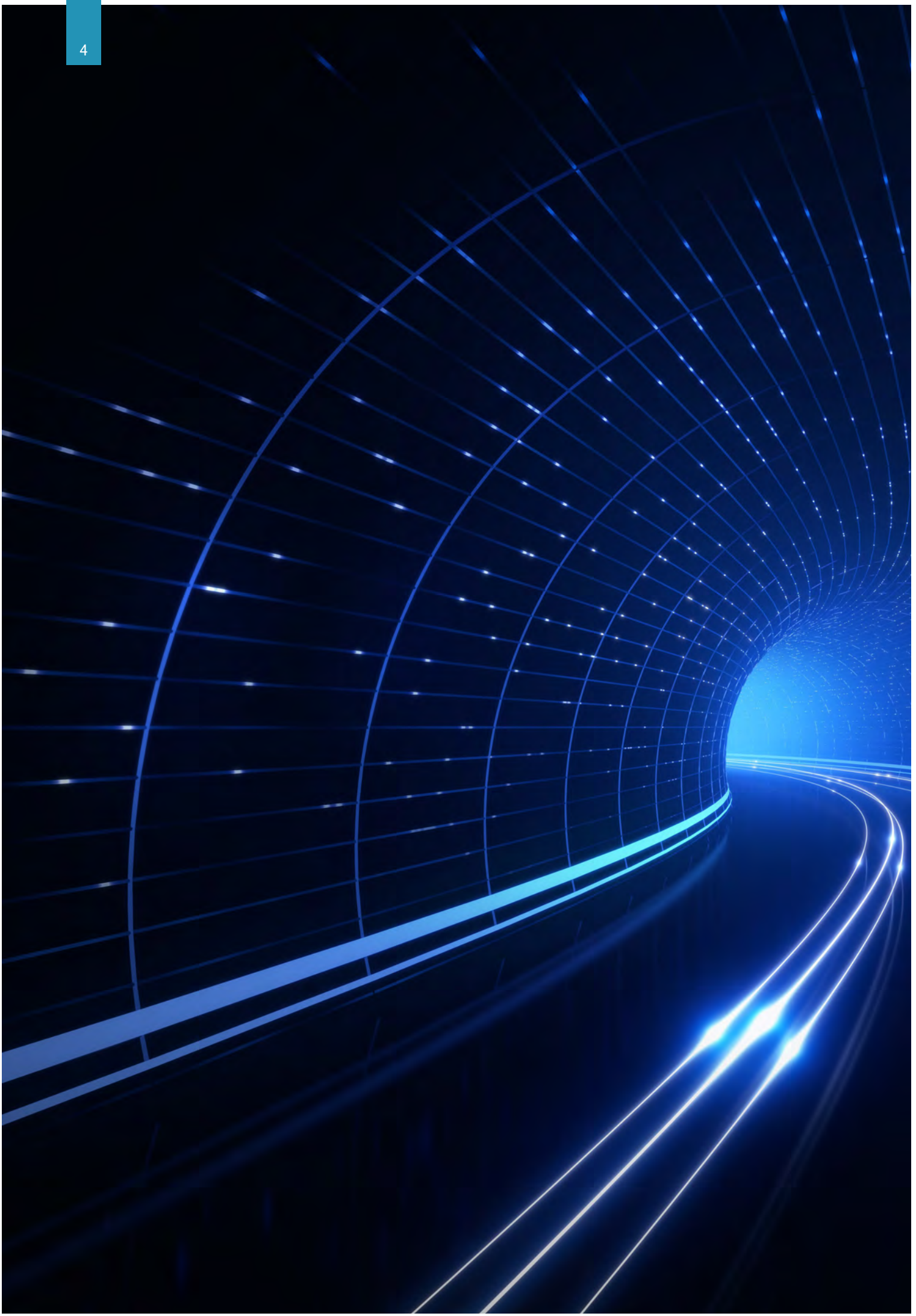
Cyber-Sicherheit in der Automobilbranche 2021/2022

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•



Inhalt



1. Einleitung

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

Dieser Bericht ist die zweite Ausgabe eines branchenspezifischen Überblicks aus Sicht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Lage der Cyber-Sicherheit im Bereich „Automotive", sowohl hinsichtlich der Produktion, als auch der Fahrzeuge selbst.

Nach wie vor sind die Auswirkungen der COVID-19-Pandemie in der Automobilbranche spürbar. Dies gilt über alle Aktivitäten hinweg, insbesondere in den Bereichen von Zulieferteilen, -produkten oder –dienstleistungen. Maßgeblich geprägt wird jedoch die Lage durch den Angriffskrieg auf die Ukraine und den damit verbundenen wirtschaftlichen, aber zunehmend auch Cyber-Sicherheitsrelevanten Auswirkungen auf die deutsche Automobilindustrie. Der Verband der deutschen Automobilindustrie (VDA) unterstützt ausdrücklich die Sanktionen der EU, welche aus wirtschaftlicher Sicht teils erhebliche finanzielle Auswirkungen für die Automobilhersteller darstellen können.

Auch in diesem Berichtszeitraum (01.07.2021 bis 30.06.2022) gilt: Cyber-Angriffe werden qualitativ immer ausgereifter und zielgerichteter. Ransomware-Angriffe sind aus Sicht des BSI weiterhin die größte operative Bedrohung der Cyber-Sicherheit, insbesondere für die IT-Systeme der Automobilhersteller und deren Zulieferer. Jedoch ist festzustellen, dass der Angriffskrieg auf die Ukraine zunehmend durch Maßnahmen im Cyber-Raum begleitet wird, welche auch Auswirkungen auf die deutsche Automobilindustrie hervorrufen und die Cyber-Sicherheit gefährden. Dies sind u.a. Verfügbarkeitsangriffe auf Webseiten durch DDoS-Angriffe sowie intensive Hacktivisten-Aktivitäten.

Das BSI gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft, als Voraussetzung einer erfolgreichen Digitalisierung. Die ganzheitliche Umsetzung dieser Aufgabe im Bereich „Automotive" ist weiterhin eine komplexe und vielfältige Herausforderung, sowohl für die Industrie als auch die zuständigen Behörden.

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. Neuregelungen für Unternehmen im besonderen öffentlichen Interesse (UBI) sollen zukünftig dabei helfen, ein breiteres Verständnis über die Cyber-Sicherheit dieser Unternehmen zu gewinnen, indem diese Informationen zu Zertifizierungen, Audits, IT-Störungen oder sonstigen Maßnahmen an das BSI übermitteln.

2. Management-übersicht zur Gesamtlage

Die Digitalisierung in modernen Autos und Verkehrsinfrastrukturen sowie in den Unternehmen der Automobilbranche schreitet weiter voran. Insbesondere der Ausbau der E-Mobilität sowie das autonome Fahren liegen als Trend-Entwicklungen im Fokus.

Durch die Digitalisierung werden neue Dienstleistungen und Funktionen im Fahrzeug ermöglicht. In dem Maße, in dem Fahrzeuge mit der Außenwelt vernetzt sind, nimmt jedoch auch die Angriffsfläche und damit die Bedeutung der Cyber-Sicherheit in der Automobilbranche weiter zu. Die dazu notwendigen, neuen Technologien dürfen nicht durch unbefugte Dritte manipulierbar sein und mögliche Cyber-Angriffe dürfen keinen Einfluss auf die Fahrsicherheit haben.

Trotz den weitreichenden Auswirkungen auf die deutsche Automobilbranche durch die COVID 19-Pandemie und durch den Angriffskrieg auf die Ukraine, muss die Umsetzung geeigneter IT-Schutzmechanismen zur Abwehr möglicher Gefährdungen weiterhin im Fokus stehen und bereits frühzeitig im Entwicklungszyklus neuer Fahrzeugmodelle berücksichtigt werden. Das Inkrafttreten und die Weiterentwicklung von neuen Standards und Normen, sollen hierzu einen entscheidenden Beitrag leisten.

Im Hinblick auf die operative Cyber-Sicherheit in den Betrieben, stellen Ransomware-Angriffe aus Sicht des BSI aktuell die größte Bedrohung dar. Zudem sind im Kontext des Angriffskrieges auf die Ukraine zunehmend Auswirkungen auf die deutsche Automobilindustrie zu beobachten, u. a. Verfügbarkeitsangriffe auf Webseiten durch DDoS-Angriffe sowie intensive Hacktivisten-Aktivitäten, welche die Cyber-Sicherheit der Unternehmen und deren Zulieferer durch Supply-Chain-Angriffe gefährden.

So wurden im Berichtszeitraum beispielsweise die folgenden, gezielten Cyber-Angriffe auf Automobilhersteller oder deren Zulieferer beobachtet:

- Cyber-Angriff auf einen deutschen Autoteilezulieferer, mit massiven Produktionsausfällen in zahlreichen Werken. Erst einen Monat später konnte die Produktion wieder weitgehend in den Normalbetrieb überführt werden.

- Ein japanischer Hersteller musste alle Autowerke in Japan stilllegen – Ein Zulieferer für Kunststoffteile war von einem Cyber-Angriff betroffen.

- Hacker haben bei einem schwedischen Hersteller Daten aus Forschung und Entwicklung erbeutet und diese im Darknet veröffentlicht. Der Datenabfluss könnte Auswirkungen auf den Geschäftsbetrieb haben.

Um den für den Wirtschafts- und Automobilstandort Deutschland wichtigen Bereich der Digitalisierung weiter sicher zu gestalten und verlässliche Rahmenbedingungen für Investitionen und Innovationen zu schaffen, arbeiten das BSI und das Kraftfahrt-Bundesamt (KBA) seit Dezember 2020 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 proaktiv durch das BSI und den Verband der deutschen Automobilindustrie (VDA) vorangetrieben.

3. Cyber-Sicherheit in der Automobil-branche

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 (EU) 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 Januar 2021 werden hier auch explizit Anforderungen an die Cyber-Sicherheit gestellt. Im Rahmen der gegenseitigen Anerkennung gilt eine erteilte Typgenehmigung in allen Unterzeichnerstaaten des Genfer Übereinkommens vom 20. März 1958.

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.

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.

2021 wurde nach vorläufigen Zahlen ein Gesamtumsatz von etwa 411 Mrd. Euro (davon 137 Mrd.

[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

Euro im Inland) erzielt. Es waren im Jahresdurchschnitt etwa 786.000 Personen in dieser Industrie beschäftigt. In Deutschland wurden 2021 ca. 3.100.000 Fahrzeuge (ohne Nutzfahrzeuge) produziert. Im Jahr 2020 haben die weltweiten Aufwendungen deutscher Unternehmen der Branche für Forschung und Entwicklung 24,5 Mrd. Euro betragen (-13,6 % zu 2019). (1)

3.2 Auswirkungen durch den Angriffskrieg auf die Ukraine

Der Angriffskrieg auf die Ukraine hat weitreichende Auswirkungen auf die Wirtschaft und die Arbeitsplätze. Lieferketten sind unterbrochen, Produktionsbänder stehen still – so auch in der Automobilbranche. Die Ukraine fällt als Produktionsstandort aus. In Werken großer Automobilhersteller stockt die Produktion, denn nach der Halbleiterkrise fehlen nun beispielsweise Kabelbäume aus der Ukraine. Fabriken mussten schließen, Logistikketten komplett umgestellt werden und auch die Energiepreise steigen zunehmend. All dies führt zu einer Knappheit entlang der gesamten Wertschöpfungskette. Ein frühzeitiges Erkennen und Managen von Risiken durch geopolitische Störungen in der Zulieferkette scheint zu wenig im Risikomanagement der Automobilhersteller, aber auch der Zulieferer, verankert zu sein.

Auch die Auswirkungen im Bereich der Cyber-Sicherheit sind spürbar. So wurden im Berichtszeitraum beispielsweise gezielte Cyber-Angriffe auf Automobilhersteller oder deren Zulieferer beobachtet. Ergänzend kamen Verfügbarkeitsangriffe durch DDoS-Angriffe sowie intensive Hacktivisten-Aktivitäten hinzu, welche die Cyber-Sicherheit der Unternehmen und deren Zulieferer (Supply-Chain-Angriffe) gefährden. Es ist wahrscheinlich, dass der Krieg in der Ukraine weiterhin von verschiedensten Formen von Cyber-Angriffen begleitet wird.

3.3 Gefahren durch Cybercrime

Nach wie vor gehen cyber-kriminelle Angriffe durch Ransomware mit einer hohen Schadenswirkung einher. Der Trend zum Big Game Hunting (zu Deutsch Großwildjagd) gegen besonders solvente Organisationen und Unternehmen hält an, auch für die Automobilbranche.

Die zunehmende Betroffenheit der Supply-Chains (Lieferketten) in der Automobilbranche durch cyber-kriminelle Angriffe, ist auch in diesem Berichtszeitraum weiterhin zu beobachten. Ziel der Täter ist es in der Regel, sensible Daten zu verschlüsseln und diese anschließend zu veröffentlichen, oder durch die Verschlüsselung den Zugang zu zentralen Serversystemen zu verhindern. Nicht verfügbare Server oder auch für die Herstellung erforderliche Datensätze, kön-

nen Ausfälle entlang der gesamten Supply-Chain nach sich ziehen. Zudem soll durch die Bekanntgabe des Opfers auf der jeweiligen Webseite der Täter, die Androhung von DDoS-Attacken sowie die gezielte Kontaktaufnahme mit Mitarbeitenden per Telefon oder E-Mail, der Druck einer Lösegeldforderung zusätzlich verstärkt werden. Denn die wichtigste Motivation von cyber-kriminellen Angriffen durch Ransomware ist der finanzielle Gewinn auf Seiten der Angreifer bzw. deren Auftraggeber.

Die Mehrheit der bekannt gewordenen Fälle, in denen Daten veröffentlicht wurden, können den beiden Ransomware-as-a-Service (RaaS) Gruppierungen BITWISE SPIDER's LockBit 2.0 und WIZARD SPIDER's Conti zugeordnet werden. Was die Anbieter von Malware-as-a-Service (MaaS) betrifft, mit Fokus auf die Automobilbranche, sind aktuell BokBot, Emotet, QakBot, Smoke Loader und ZLoader zu verzeichnen.

Im Berichtszeitraum wurden im Kontext des Big Game Hunting zudem verstärkt neue Linux-basierte Varianten von Ransomware beobachtet, welche insbesondere auf die Deaktivierung und Verschlüsselung von virtuellen Maschinen (VMs) spezialisiert sind, welche auf ESXi Virtualisierungsplattformen betrieben werden.

Maßnahmenempfehlungen

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., haben im Fall von Ransomware ein hohes und unmittelbares Schadenpotential.

Auch das Verhalten der Mitarbeitenden spielt eine zentrale Rolle. Einige Angriffe wirken 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 Mitarbeitenden helfen.

Zur Prävention vor DDoS-Attacken ist die Etablierung geeigneter Mitigationsmaßnahmen sinnvoll.

Hierzu stellt das BSI eine Liste qualifizierter Dienstleister zur Verfügung.

3.4 Bedeutung der Informationssicherheit in der Supply Chain

Ausgehend von den o.g. Gefahren durch cyberkriminelle Angriffe und der aktuell vorherrschenden Bedrohungslage im Kontext des Angriffskrieges auf die Ukraine, sind verstärkt Angriffe im Bereich der Automobilzulieferer zu beobachten. Die enge Verzahnung und daraus resultierende Abhängigkeit der Automobilhersteller von einer – oftmals just-in-time – funktionierenden Zulieferkette, haben schnell massive Auswirkungen auf die gesamte Wertschöpfungskette, auch wenn nur ein einzelner Zulieferer ausfällt.

Im Berichtszeitraum waren mehrere Vorfälle von Produktionsausfällen bei Zulieferern zu beobachten. Ein weltweit führender Autohersteller beispielsweise, musste alle Werke in seiner Heimat in Folge eines Cyber-Angriffs stoppen und die Produktion vorübergehend einstellen. Der Hersteller war offenbar nicht mehr in der Lage, die benötigten Teile rechtzeitig zu erhalten. Die Ursache dafür lag allerdings nicht auf Seiten des Herstellers, sondern ein wichtiger Zulieferer war Opfer eines massiven Ransomware-Angriffs geworden und konnte die Produktion nicht mehr aufrechterhalten.

3.5 Qualifizierung von Schlüsselpersonal

Die Fahrzeuge der Zukunft kommen nicht nur ohne fossile Kraftstoffe aus, sie sind auch vernetzt und automatisiert unterwegs. Außerdem müssen die Wertschöpfungsketten nachhaltiger und robuster werden. Wichtig dafür ist auch eine eigenständige und leistungsfähige Produktion für zentrale Bestandteile der Autos in Deutschland und Europa – vorneweg für Chips und Batterien.

Gut ausgebildete Fachkräfte sind daher eine wichtige Voraussetzung für den Erhalt und die Weiterentwicklung der Innovations- und Wettbewerbsfähigkeit der deutschen Automobilindustrie. Angesichts des demografischen Wandels ist die Sicherung des Fachkräftebedarfs eine der großen Herausforderungen der kommenden Jahre. Die berufliche Bildung ist eine wichtige Grundlage und Voraussetzung, um den Fachkräftebedarf langfristig zu decken. Durch die unmittelbare Nähe zur betrieblichen Praxis bietet die Berufsausbildung beste Voraussetzungen für den Übergang ins Arbeitsleben und eröffnet darüber hinaus vielfältige Karriere- und Entwicklungschancen.

Der Expertenkreis „Transformation der Automobilwirtschaft“, unter Federführung des Bundministeriums für Wirtschaft und Klimaschutz (BMWK), ist Teil der im Koalitionsvertrag vorgesehen Strategieplattform, die sich mit der Transformation der Automobil- und Mobilitätswirtschaft befasst. Er soll konkrete Handlungsempfehlungen erarbeiten, wie das Ziel der Klimaneutralität erreicht und Wertschöpfung sowie Arbeits- und Ausbildungsplätze am Automobilstandort Deutschland gesichert werden können. Digitalisierung und Stärkung der Liefernetzwerke sind zentrale Herausforderungen und zugleich die Chancen der Automobilwirtschaft in Deutschland. Die konstituierende Sitzung des Expertenkreises fand dazu im Juni 2022 statt.

4. Cyber-Sicherheit im Fahrzeug sowie in digitalen Produkten

Die Digitalisierung bleibt neben der Elektromobilität ein bestimmendes Thema für die Automobilbranche. Die Cyber-Sicherheit der Fahrzeugsysteme ist dabei eine Schlüsseleigenschaft für eine erfolgreiche Umsetzung. Durch die neu eingeführten Regelungen zur Cyber-Sicherheit (siehe Kapitel „Regulierung und Standardisierung – Vorgaben zur Cyber-Sicherheit“) sind die Hersteller verpflichtet, Cyber-Sicherheit zukünftig in der Produktentwicklung zu berücksichtigen und ein Cyber-Sicherheitsmanagement aufzubauen, so dass im Fall von neu auftretenden Schwachstellen schnell Gegenmaßnahmen umgesetzt werden können.

4.1 Vernetztes Fahren

Die Anfälligkeit von Fahrzeugsystemen, die über eine Funkverbindung verfügen oder mit Hintergrundsystemen vernetzt sind, wurde durch verschiedenen Forschungsarbeiten und Vorfälle im Berichtszeitraum verdeutlicht. Nachfolgend sind einige Beispiele aufgeführt.

Ausfall von Infotainmentsystemen durch fehlerhafte Meta-Daten

Der Radiosender KUOW Seattle sendete in seinen Meta-Daten Bilder, für die Anzeige im Infotainmentsystem eines Fahrzeuges, ohne die korrekte Angabe des Dateiformates. Bestimmte Infotainmentsysteme in Fahrzeugen der Jahrgänge 2014-2017 scheiterten beim Parsen der Daten, offenbar ohne eine Möglichkeit, sich von dem Fehler zu erholen. Dies führte dazu, dass das

System in einen sogenannten „Boot-Loop“ geriet, der das Infotainmentsystem für den Anwender unbrauchbar machte. Tatsächlich musste das 1500$ teure System ersetzt werden (2).

Fehler beim Verarbeiten von Zeichenketten sind in der Regel auf einfache Programmierfehler zurückzuführen. Gerade Systeme die mit speicherunsicheren Programmiersprachen wie C und C++ programmiert wurden, müssen bei der Entwicklung sorgfältig getestet werden. Solche Fehler, die zum Absturz eines Systems führen, können als Schwachstellen gewertet werden, da diese auch mutwillig von einem Angreifer ausgenutzt werden können.

Bereits zuvor wurde eine derartige Schwäche in einem anderen Infotainmentsystem ausfindig gemacht (3), welche ebenfalls auf einen typischen Programmierfehler zurückzuführen ist. Funktionen zur Verarbeitung von Zeichenketten können heutzutage mit modernen Open-Source-Fuzzern effektiv getestet werden. Einige Infotainmentsysteme auf dem Markt erlauben das Steuern von Komfortfunktionen, das Öffnen des Wagens oder bieten sogar Zugriff auf die Scheibenwischer. Darüber hinaus fließen viele, möglicherweise auch personenbezogene Daten durch dieses System. Daher sollte auch die Sicherheit von Infotainmentsystemen nicht vernachlässigt werden.

Öffnen von Fahrzeugen durch ungesicherte API-Token[3]

Anfang des Jahres entdeckte ein Sicherheitsforscher eine Fehlkonfiguration im Open Source Projekt „TeslaMate“ (4). Hierbei handelt es sich um eine Datenlogging-Plattform, welche über die Web-API des Fahrzeugherstellers verschiedene Daten über das Auto eines Nutzers sammelt und visualisiert. Der Hersteller stellt diese Web-API seinen Kunden zur Verfügung. Für die Nutzung ist allerdings eine entsprechende Authentifizierung mit einem API-Token erforderlich.

Durch den Angriff war ein Zugriff auf API-Token möglich, die verwendet werden konnten, um diverse Funktionen von über 25 Wagen zu steuern. Eine selbst gehostete TeslaMate-Instanz, basierend auf der mitgelieferten Standardkonfiguration, speicherte die verwendeten API-Token zusammen mit den anderen Daten im Klartext in einer Postgres-Datenbank ab. Auf diese Datenbank konnte dann über das mitverbaute „Grafana“, einer weiteren Open-Source Software, zugegriffen werden. Die so extrahierten API-Token konnten verwendet werden, um über das Internet diverse Fahrzeugfunktionen zu steuern, wie etwa das Öffnen und Schließen des Wagens, oder das Starten des Motors. Außerdem konnten sensible Daten, wie die Position des Autos erfasst werden. Der Fall ist insofern interessant, als dass hier keine direkte Schwachstelle in den Autos selbst bestand. Die API

[3] Ein API-Token ist ein einzigartiges Datum, welches den Besitzer gegenüber einer Schnittstelle identifiziert und ihn bemächtigt, die Schnittstelle in einem definierten Rahmen zu nutzen.

stellt eine gewollte Funktionalität dar, die auch von vielen Fahrzeugbesitzern geschätzt wird. Jedoch veröffentlichten Nutzer von TeslaMate unwissentlich und unbeabsichtigt ihre Authentifizierungsdaten im Internet. Dies entzieht sich weitestgehend der Kontrolle des Herstellers. Dieser kann lediglich darauf hinarbeiten, die Kontrolle über Authentifizierungsdaten möglichst einfach zu gestalten. Die Fahrzeugnutzenden müssen sich bewusst sein, dass auch über Software (oder Hardware) von dritter Seite Gefährdungen auftreten können. Datenzugriffe und die Ausführung von Fahrzeugfunktionen sind prinzipiell zwei separate Anwendungsfälle. Dies könnte sich in der Authentifizierung, etwa über Token die unterschiedlichen Rechte repräsentieren, widerspiegeln.

Replay Angriffe auf Schließsysteme

Elektronische Schließsysteme sind weiterhin ein beliebtes Forschungsobjekt für Sicherheitsforschende. Neben etwa einem neuartigem Relay-Angriff über Bluetooth Low Energy (5), oder einer Schwäche in einer Schlüsselkartenregistrierung (6), fanden die Sicherheitsforschenden Blake Berry und Ayyappan Rajesh mit CVE-2022-27254 eine Schwäche in einem Schließsystem, die es erlaubt ein Schlüsselsignal aufzunehmen und fortan beliebig oft wiederzuverwenden (7). Diese Replay-Angriffe wurden bereits in den neunziger Jahren seitens der Hersteller als Problem identifiziert und durch die seither viel verwendeten Rolling Codes mitigiert. In der Regelung 116 der UNECE von 2012 werden diese Rolling Codes auch explizit gefordert. Scheinbar wird allerdings auch in modernen Modellen anfällige Technologie für den Remote Keyless Entry weiterhin verbaut.

Das KBA und das BSI haben in dieser Sache ein vermeintlich betroffenes Modell untersucht und stellten fest, dass hier ein Rolling Code verwendet wird. Der Hersteller teilte dem KBA bereits zuvor auf Anfrage hin mit, dass sich die technischen Spezifikationen europäischer Modelle von den amerikanischen unterscheiden und daher europäische Modelle nicht betroffen seien.

Eine Vielzahl elektronischer Schließsysteme weisen signifikante Schwächen auf. Der ADAC kommt auch dieses Jahr wieder zu dem Ergebnis, dass ein großer Teil der sich im Markt befindenden Autos anfällig gegenüber sogenannten Relay-Angriffen ist (8), bei denen ein Angreifer den Funkkanal zwischen Auto und Schlüssel verlängert und somit die heute weit verbreitete Passive Keyless Entry Funktionalität ausnutzt, um ein Auto zu öffnen und in manchen Fällen sogar zu starten.

Hoffnungsträger ist die neue Ultrawideband-Technologie, die immer mehr Einzug in den Markt findet. Mithilfe dieser Technologie lässt sich die tatsächliche Position des Fahrzeugschlüssels äußerst genau bestimmen, was Relay Angriffe in der Form, wie sie bisher existierten, voraussichtlich unmöglich macht.

Unterbrechung von Schnellladevorgängen

Auch im Zuge des Hochlaufs der Elektromobilität werden zunehmend Schwachstellen erkannt. Im Rahmen einer Forschungsarbeit (9) wurde eine Schwachstelle im Combined Charging System (CCS), einem weit verbreiteten Ladestandard für batterieelektrische Fahrzeuge, entdeckt. Ziel des Angriffs ist die Unterbrechung eines Ladevorganges von einem oder mehreren Elektrofahrzeugen. Es handelt sich um einen Angriff auf die im CCS verwendete Kommunikationstechnologie Power Line Communication (PLC). Der CCS-Standard wird in Ladesystemen für eine Vielzahl von Transportsystemen (LKW, Busse, Fähren, Flugzeuge, etc.) angewendet sowie perspektivisch auch in Netzanwendungen. Die Schwachstelle ist nur für das Schnellladen (DC-Charging) relevant. Da die ausgetauschten Informationen sicherheits- und steuerungsrelevant sind, wird bei einer Störung der Kommunikation der Ladevorgang abgebrochen. Dieses Verhalten ist von den einschlägigen Standards vorgegeben. Dies wird bei dem Angriff ausgenutzt und die Steuerkommunikation zwischen Elektrofahrzeug und Ladegerät durch Funksignale derart gestört, dass es zu einem Verbindungsabbruch zwischen Ladesäule und dem aufzuladen-

den Elektrofahrzeug kommt. Für einen vollständigen Paketverlust der PLC-Kommunikation reiche laut Autoren eine Sendeleistung von 10mW, um 10 Meter Abstand (in einer Laborumgebung) zu überwinden, bei höheren Sendeleistungen können bis zu 47 Meter erreicht werden.

Die Auswirkungen eines Angriffs bleiben glücklicherweise überschaubar, da hierbei kein bleibender Schaden am Fahrzeug oder Ladegerät entsteht. Durch das beschriebene Szenario könnte aber die Verfügbarkeit des Ladens bei öffentlich zugänglichen Schnelladesäulen lokal eingeschränkt werden. Ein Angreifer muss über das notwendige Equipment verfügen (welches allerdings relativ leicht zu beschaffen ist) und sich in der Nähe des Angriffsziels befinden.

Als Gegenmaßnahme empfehlen die Autoren, eine automatische Wiederaufnahme des Ladevorgangs nach einer Störung im Protokoll umzusetzen, so dass der aufgezeigte Störangriff nicht zu einer andauernden Unterbrechung führt. Das Beispiel macht deutlich, dass gerade im Automobilbereich Risiken aus Sicht der Betriebssicherheit gegen Risiken bezüglich der Cyber-Sicherheit abgewogen und im Systementwurf berücksichtigt werden müssen. Fragen der Cyber-Sicherheit sollten daher bereits in der Standardisierung entsprechender Systeme mitgedacht und adressiert werden.

4.2 Automatisierung und Künstliche Intelligenz

Wie schon in den vergangenen Jahren schreitet die Entwicklung im Bereich des automatisierten Fahrens weiterhin voran. Diese stützt sich in erster Linie auf gesteigerte Rechenleistung und Datenmengen, auf deren Basis KI-Verfahren stetige Fortschritte machen. Neben der Umsetzung neuer Funktionalitäten und steigender Performanz schafft die Nutzung von KI-Verfahren im automatisierten Fahren jedoch auch neue Herausforderungen, denen für einen sicheren Einsatz begegnet werden muss. Hierzu zählen beispielsweise neuartige Angriffe sowie die erforderliche robuste Funktionsweise unter vielfältigen Umweltbedingungen. Von besonderer Bedeutung sind dabei anerkannte Kriterien, um die Voraussetzungen für einen sicheren Einsatz der KI-Verfahren zu überprüfen. Geeignete Konzepte und Methoden sind jedoch bisher nicht verfügbar oder nicht ausgereift.

Diesem Themenkomplex widmet sich das Projekt AIMobilityAuditPrep (10), das seit Dezember 2021 vom BSI mit dem Technologieunternehmen ZF und der TÜV Informationstechnik GmbH (TÜViT) durchgeführt wird. Ziel des Projekts ist die Erprobung und Weiterentwicklung von Anforderungen, Methoden und Werkzeugen für den Bereich des automatisierten Fahrens. In einem Folgeprojekt, dessen Start für den Herbst 2022 geplant ist, sollen diese Vorarbeiten anhand zweier Anwendungsfälle aus dem automatisierten Fahren umfangreich getestet und konkretisiert werden. Mittelfristig plant das BSI, auf Basis der gewonnenen Erkenntnisse eine modulare technische Richtlinie zu erstellen.

Des Weiteren bringt das BSI diese Erkenntnisse auch aktiv in internationalen Regulierungs- und Standardisierungsvorhaben ein. In diesem Bereich gab es im vergangenen Jahr ebenfalls verstärkte Aktivitäten. So sieht die geplante KI-Verordnung der EU weitreichende Anforderungen an sicherheitskritische KI-Systeme (wie im Bereich des automatisierten Fahrens) vor. Auch in der UNECE, deren Regelungen im Kontext der Typgenehmigung von Fahrzeugen eine wichtige Rolle spielen, wurde zuletzt vermehrt über KI-Systeme im automatisierten Fahren diskutiert. Perspektivisch sollen diese Diskussionen verstetigt werden.

5. Cyber-Sicherheit in Produktions-anlagen und -prozessen

Neben einer Absicherung der Automobile selbst, stellt der Schutz der Produktionsanlagen und –prozesse eine wesentliche Herausforderung dar, wobei es Überschneidungen der beiden Bereiche gibt.
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 die Angriffsfläche, da diese Systeme auch an das Unternehmensnetzwerk und Dienstleister-Netzwerke angeschlossen sein können und teilweise über das Internet erreichbar sein sollen.

5.1 Digitalisierung als Herausforderung in der Produktion

Die Trends, die sich in den letzten Jahren durch die Digitalisierung der Produktion abgezeichnet haben, setzen sich weiter fort. Insgesamt haben sich die daraus entstehenden Gefährdungen nicht verändert und sind bekannt.

Aufgrund der allgemeinen Professionalisierung der Angreifer und dem breiten Einsatz von Ransomware ist vermehrt zu beobachten, dass auch Produktionsanlagen hiervon betroffen sind. Sei es durch Beeinträchtigungen der Office-Systeme und damit fehlenden Auftragsdaten, oder eine direkte Betroffenheit von Systemen in den Produktionsanlagen. Die Beeinträchtigung der Produktion ist meist eine Folge des Ransomware-Angriffs.

Neben der allgemeinen Gefahr durch Ransomware-Angriffe, gibt es immer wieder Beispiele für Schadsoftware, die spezifisch auf industrielle Steuerungsanlagen (ICS[4]) ausgerichtet sind. Diese haben das Ziel, Informationen zu sammeln oder Manipulationen vorzunehmen. Dies reicht von der Energieerzeugung und -verteilung über die Gas- und Wasserversorgung, bis hin zur Fabrikautomation, Verkehrsleittechnik und modernem Gebäudemanagement. Ein allgemeines Beispiel ist die Schadsoftware Industroyer2, welche in der Ukraine im Frühjahr 2022 entdeckt wurde. Das Risiko und Schadenspotenzial von sowohl nicht-zielgerichteter Schadsoftware, als auch von gezielten, qualitativ hochwertigen und mit signifikantem Aufwand durchgeführten spezifischen Angriffen gegen industrielle Steuerungsanlagen, muss berücksichtigt werden. Dies gilt sowohl für Systeme, die unmittelbar mit dem Internet verbunden sind, als auch für diejenigen, welche auf mittelbarem Wege durch Cyber-Angriffe attackiert werden können.

Grundsätzlich besteht ebenfalls weiterhin die Gefahr, dass Zulieferer und Dienstleister angegriffen werden und dass sich daraus Auswirkungen für die Produktionsumgebungen ergeben können. Vereinzelt kam es durch Ransomware-Angriffe zu Beeinträchtigungen in der Lieferkette. Dies spiegelt sich auch in den im Frühjahr 2022 aktualisierten „ICS TOP 10 Bedrohungen und Gegenmaßnamen“ (11) wieder.

5.2 Schwachstellenmanagement

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.

[4] Industrial Control System

Als prominentes Beispiel, verdeutlicht die Schwachstelle Log4j die Bedeutung von Softwarequalität für die Cyber-Sicherheit, im Kontext eines funktionierenden Schwachstellenmanagements. Die Verbesserung der Softwarequalität ist ein wichtiger Beitrag zur Erhöhung der Cyber-Sicherheit, als Grundlage einer erfolgreichen Digitalisierung.

Softwarehersteller sollten daher im eigenen Interesse daran (mit)arbeiten, schnellstmöglich und konsequent herstellerseitig einen Prozess zum Umgang mit Meldungen über Schwachstellen in ihren IT-Produkten und Systemen zu etablieren, einen sogenannten Coordinated Vulnerability Disclosure (CVD)-Prozess. Dieser ermöglicht es Sicherheitsforschenden, die Schwachstellen in IT-Produkten entdeckt haben, diese an eine zentrale Adresse zu melden und bei der Behebung und geeigneten Veröffentlichung von Patches zu unterstützen. Große CVD-Fälle haben gezeigt, dass viele Hersteller nur mit sehr viel Mühe feststellen können, welche Bibliotheken und andere Dritthersteller-Software in ihren Produkten und über die gesamte Wertschöpfungskette hinweg eingesetzt werden. Das BSI fordert daher eine zielgerichtete Umsetzung von Maßnahmen für eine bessere Softwarequalität in IT-Produkten. Dazu unterstützt das BSI aktiv Konzepte wie beispielsweise Software Bill of Materials (SBOM)[5] und Common Security Advisory Framework (CSAF)[6], um CVD-Prozesse zu optimieren.

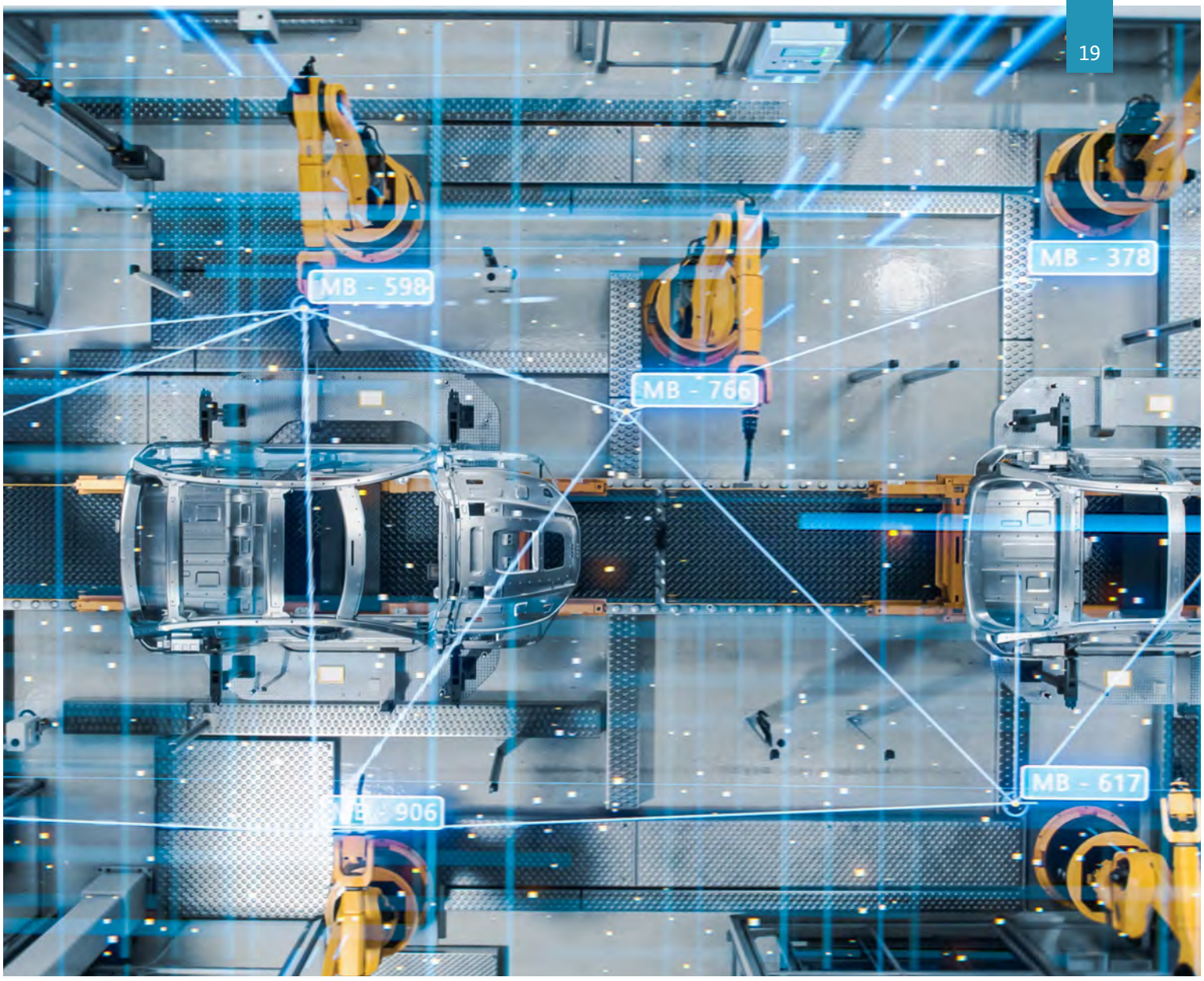
Verantwortung kommt auch den Anwenderunternehmen zu: So haben auch die Automobilhersteller einen aktiven Part dabei, ihre eigenen IT-Systeme und Netze im Rahmen eines geeigneten Schwachstellenmanagement-Prozesses zu schützen. Wer das nicht tut, geht enorme Risiken ein, denn Produktionsausfälle infolge eines Cyber-Angriffs können schnell existenzbedrohend sein. Gemäß dem Motto des diesjährigen Cyber-Sicherheitskongresses muss Cyber-Sicherheit daher Chefinnen- und Chefsache sein und mit ausreichenden Ressourcen zum festen Bestandteil des eigenen Risiko-Managements gemacht werden.

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.

Zu den Funktionen und Diensten, die durch Algorithmen realisiert werden, gehören weiterentwickelte Fahrassistenten, autonome Fahrfunktionen und natürlich die Konnektivität. Ein großer Teil der Wertschöpfung wird zukünftig durch solche Dienste erzielt. Eine international durchgeführte Studie (12) zeigt jedoch: Noch fehle die Reife bei der Software. Rund die Hälfte der deutschen Unternehmen stecken in der Anfangsphase, wenn es um eigene Software-Plattformen geht. Neue Software gibt es im Abstand von wenigen Wochen, ein komplett neues Automodell wird hingegen ca. alle acht Jahre entwickelt und produziert. Gemäß der Studie nutzen über 90 Prozent der großen Hersteller eine traditionelle Fahrzeugarchitektur. Und nur rund 10 Prozent planen, die Hard- von der Softwarearchitektur zu entkoppeln. Im Bereich Connected Cars entwickeln verschiedene Anbieter spezielle Sicherheitslösungen für vernetzte Fahrzeuge. Diese sollen Automobilhersteller dabei unterstützen, die aktuellen Cyber-Sicherheitsvorschriften für die Branche umzusetzen.

[5] In einer SBOM werden alle Abhängigkeiten einer Software aufgelistet, um eine effiziente Überprüfung zu ermöglichen, ob eine bekannte Schwachstelle ein Produkt betrifft.
[6] Ein maschinell verarbeitbares Format für Security Advisories.



Der Markt für vernetzte Fahrzeuge wächst rapide und Daten über Fahrzeuge und die sie umgebenden Verkehrsbedingungen spielen eine immer größere Rolle bei der Entwicklung zukunftsfähiger Mobilitätslösungen. Aufgrund ihrer Verbindung zum Internet sind intelligente Fahrzeuge jedoch der Bedrohung durch Cyber-Angriffe ausgesetzt. Deshalb ist eine kontinuierliche Sicherheits- und Bedrohungsüberwachung in den vernetzten Fahrzeugen selbst, sowie über die Plattform hinweg erforderlich, um Vorfälle und Anzeichen von Cyber-Angriffen zuverlässig zu erkennen und darauf zu reagieren. Nur so gelingt ein umfassender Überblick über die Fahrzeugdaten. Eine Lösung, die in der Lage ist, viele weltweit eingesetzte Fahrzeuge gegen die ständig wachsenden Angriffe zu überwachen und abzusichern, erfordert eine sorgfältige Koordination zwischen Cloud-Security, IT-Systemen und Automobilinfrastruktur.

Hinsichtlich der Vertrauenswürdigkeit stehen viele Unternehmen weiterhin vor der Frage, wie diese zu bewerten ist und wie eine sichere Anbindung für Fernservices realisiert werden kann. Im Rahmen des IT-Grundschutzes wurde der neue Baustein „IND Fernwartung in Produktionsumgebungen“ (13) veröffentlicht. In diesem werden Anforderungen für den Zugriff durch Dienstleister auf die Produktionsumgebung aufgelistet. Darüber hinaus hat sich der C5-Standard des BSI (14), insbesondere bei Cloud-Anbietern weiter etabliert und kann ebenfalls genutzt werden.

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) in Fragen der Cyber-Sicherheit eng zusammen. Mit neuen Regeln für die Genehmigung von Fahrzeugen sollen beispielsweise das Thema Cyber-Sicherheit über den gesamten Lebenszyklus eines Fahrzeuges fest verankert und Risiken besser vorgebeugt werden. Der für den Transfer in die Anwendung erforderliche Austausch mit der Automobilindustrie wird dabei auch proaktiv durch das BSI und den Verband der deutschen Automobilindustrie (VDA) vorangetrieben.

6.1 Informationssicherheit im Unternehmen

Im Kontext der weiter stark zunehmenden Vernetzung und Globalisierung der Informationssysteme, ist ein vergleichbares Informationssicherheitsniveau aller Beteiligten, über die gesamte Wertschöpfungskette hinweg, von entscheidender Bedeutung. Vergleichbarkeit entsteht jedoch nur, wenn vergleichbare Cyber-Sicherheitsstandards genutzt werden. Das Branchenmodell TISAX ist solch ein IT-Standard innerhalb der Automobilbranche. Basierend auf dem VDA Information Security Assessment (ISA) Katalog, gewährleistet TISAX eine unternehmensübergreifende Anerkennung von Assessment-Ergebnissen. TISAX existiert aktuell in der Version 5.1. Mehr als 2.800 Unternehmen der Automobilbranche haben sich seit 2017 für TISAX registriert. Es ist davon auszugehen, dass weitere Automobilhersteller sich dem anschließen werden.

6.2 Regulierung und Standardisierung – Vorgaben zur Cyber-Sicherheit

Die regulativen Vorgaben zur Cyber-Sicherheit in Kraftfahrzeugen gemäß der UNECE-Regelung UN-R155 (15) und der Verordnung (EU) 2018/858 müssen seit Juli 2022 von den Herstellern verpflichtend für alle neuen Fahrzeugtypen umgesetzt werden.

Im August 2021 wurde der Standard ISO/SAE 21434 „Road Vehicles - Cybersecurity Engineering“ veröffentlicht. Dieser Standard richtet sich an Fahrzeughersteller und definiert einen Rahmen für die Umsetzung von Cyber-Sicherheitsanforderungen in der Entwicklung von Fahrzeugen. Ähnlich wie die UN-R 155 betrachtet der Standard die Konzept-, Produktentwicklungs- und Nach-Entwicklungsphase für das Fahrzeug und legt für jede Phase entsprechende Aufgaben fest.

Ein wesentlicher Bestandteil der Konzeptphase ist die Bedrohungsanalyse und Risikobewertung (engl. threat analysis and risk assessment, kurz TARA). Hierfür werden in der ISO/SAE 21434 folgende Schritte festgelegt: Identifikation der schützenswerten Güter („assets“), Identifikation von Bedrohungsszenarien, Bewertung der Auswirkungen eines Bedrohungsszenarios, Angriffspfadanalyse, Bewertung der Durchführbarkeit von Angriffspfaden, Risikobestimmung und Entscheidung über die Risikobehandlung. Für die einzelnen Schritte wird keine konkrete Methodik festgelegt, sondern es wird ein Rahmen definiert, der grobe Vorgaben, wie etwa die zu verwendenden Kategorien, zur Bestimmung der Bedrohungsauswirkungen und Risikoskalen enthält.

Für die Produktentwicklungsphase werden Anforderungen für die schrittweise Verfeinerung der Cyber-Sicherheitsspezifikation auf Grundlage

der TARA und für die Verifikation der Implementierung formuliert. Um zu verhindern, dass neue Risiken in der Verfeinerung und durch die Interaktion verschiedener Komponenten entstehen, ist eine Schwachstellenanalyse in dieser Phase vorgeschrieben. Ebenso ist eine Prüfung der Implementierung, z.B. mit Hilfe von Interface-Tests oder einer Code-Analyse vorgesehen. Ferner werden Anforderungen an die Softwareentwicklung (Verwendung von Richtlinien zur sicheren Entwicklung) definiert.

In der Nach-Entwicklungsphase muss gemäß dem Standard ISO/SAE 21434 insbesondere eine Vorfallsbearbeitung (incident response) stattfinden, die sicherstellt, dass alle Betroffenen in geeigneter Weise z.B. über eine neu aufgetretene Schwachstelle informiert werden und dass passende Gegenmaßnahmen entwickelt und ausgerollt werden.

Dieser Standard bezieht explizit über die Lieferkette verteilte Aktivitäten zur Cyber-Sicherheit ein. Beispielsweise sollen die Fähigkeiten zur Umsetzung von Cyber-Sicherheitsaktivitäten bei Zulieferern evaluiert werden. Weiterhin wird gefordert, dass entsprechende Vereinbarungen (Cybersecurity Interface Agreements) zwischen Hersteller und Zulieferer geschlossen werden.

Die Anwendung des Standards kann bei der Umsetzung der regulatorischen Anforderungen unterstützen. Ein Nachweis der Umsetzung der ISO/SAE 21434 ist aber weder formale Voraussetzung für die Erfüllung der UNECE-Regelung UN-R155, noch ist der Standard deckungsgleich mit den Anforderungen der Regulierung.

Seit dem März 2022 existiert die Spezifikation ISO/PAS 5112:2022 „Road Vehicles - Guidelines for auditing cybersecurity engineering“. Diese stellt eine Richtlinie zur Durchführung von internen oder externen Audits für Cyber Security Management Systeme auf Grundlage der ISO/SAE 21434 dar. Die Spezifikation formuliert An-

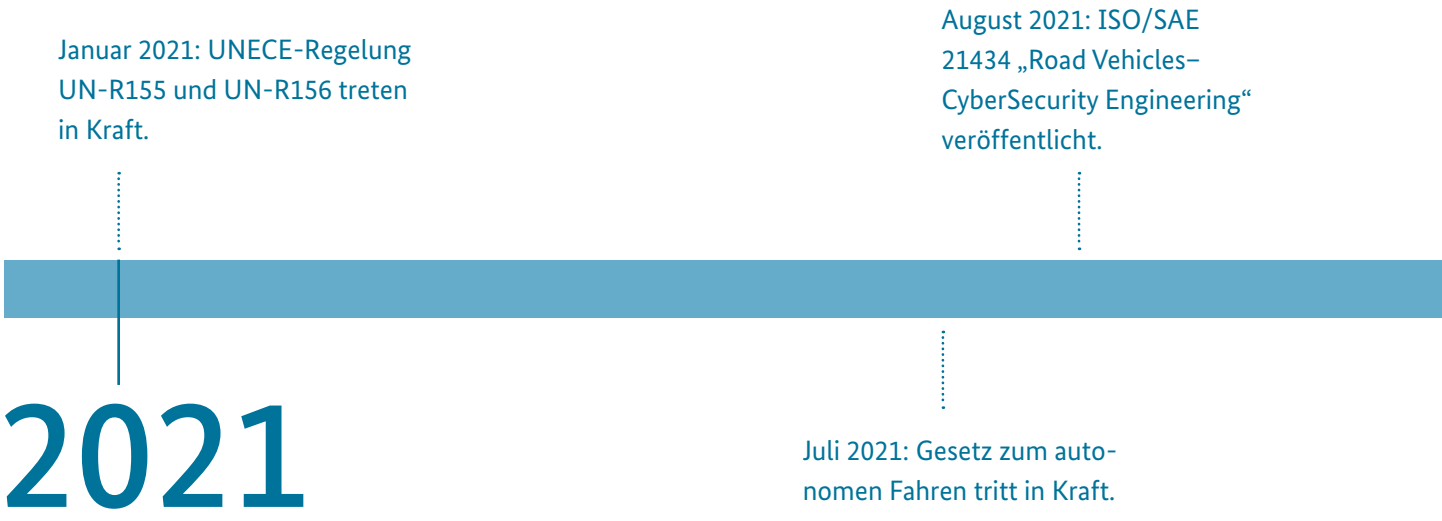


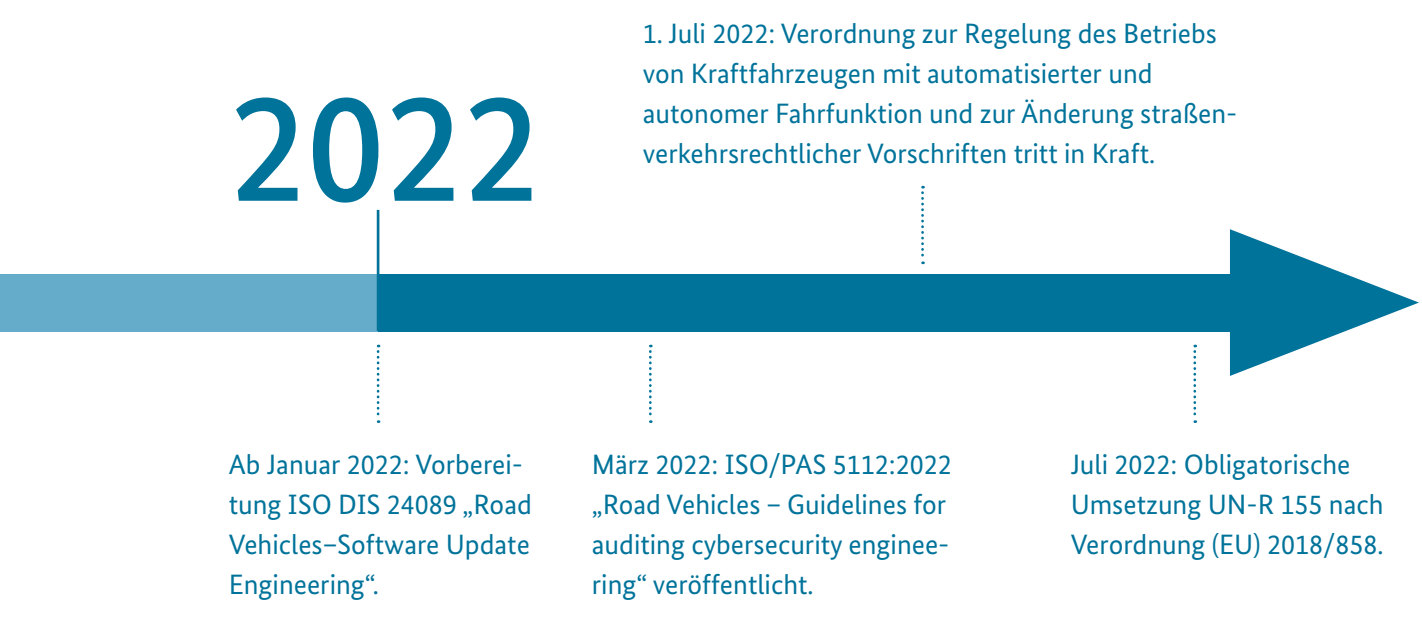
Abbildung: Zeitleiste Regulierung und Standardisierung mit Relevanz für die Cyber-Sicherheit in Fahrzeugen

forderungen an das Management des Auditprogramms, an die eigentliche Durchführung und an die Kompetenz der Auditorinnen und Auditoren.

Parallel zur oben genannten Regelung ist die UNECE-Regelung UN-R156 zu Software Updates und Software Update Management Systemen Anfang 2021 in Kraft getreten. Derzeit in Entwicklung befindet sich der Standard ISO/DIS 24089 „Road Vehicles – Software Update Engineering". Ähnlich wie der oben genannte Standard bei der Umsetzung der UNECE-Regelung UN-R155 helfen kann, soll der ISO 24089 die Umsetzung der regulatorischen Anforderungen aus der UNECE-Regelung UN-R156 unterstützen. Auch dieser Standard sieht eine explizite Betrachtung von Cyber-Sicherheitsrisiken im gesamten Update-Prozess vor. Dies beinhaltet u.a. die Sicherheit des Update-Mechanismus im Fahrzeug selbst, einschließlich der dafür notwendigen Konfigurationsinformationen, aber auch die sichere Verwaltung der Softwarepakete auf Infrastrukturseite.

Am 1. Juli 2022 trat die Verordnung zur Regelung des Betriebs von Kraftfahrzeugen mit automatisierter und autonomer Fahrfunktion und zur Änderung straßenverkehrsrechtlicher Vorschriften in Kraft. Diese Verordnung ergänzt das Gesetz zum autonomen Fahren, welches am 28. Juli 2021 in Kraft getreten ist und regelt u.a. das Verfahren für die Erteilung einer Betriebserlaubnis für entsprechende Kraftfahrzeuge.

Der Hersteller ist nach dieser Verordnung verpflichtet, die Anforderungen der UNECE-Regelung UN-R155 zu erfüllen und insbesondere die notwendigen Funkverbindungen der Fahrzeuge zu den Hintergrundsystemen nach Stand der Technik abzusichern.



6.3 Neuregelungen für Unternehmen im besonderen öffentlichen Interesse (UBI)

Mit dem Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0), ergeben sich neue Regelungen für Unternehmen im besonderen öffentlichen Interesse (UBI). Diese Neuregelungen gelten auch für mehrere Automobilfirmen. Das betrifft besonders Unternehmen, die aufgrund ihrer inländischen Wertschöpfung zu den Größten in Deutschland gehören. Als Grundlage dient die Top-100-Liste der umsatzstärksten deutschen Unternehmen. Diese werden zusätzlich verpflichtet, alle zwei Jahre eine Selbsterklärung zur Cyber-Sicherheit an das BSI abzugeben. Darin müssen sie unter anderem angeben, welche Zertifizierungen, Audits oder sonstigen Maßnahmen sie durchführen.

Die konkreten Pflichten für UBI sind in § 8f BSIG aufgeführt. Welche Unternehmen UBI sind, ist in § 2 Absatz 14 BSIG definiert.

Es gibt drei Kategorien von UBI:

- UBI 1 (AWV-UBI) sind Hersteller / Entwickler von Gütern im Sinne von § 60 Außenwirtschaftsverordnung (AWV), also Unternehmen, die im Bereich Waffen, Munition und Rüstungsmaterial oder im Bereich von Produkten mit Cyber-Sicherheitsfunktionen zur Verarbeitung staatlicher Verschlusssachen oder für die Cyber-Sicherheitsfunktion wesentlicher Komponenten solcher Produkte tätig sind.
- UBI 2 (Wertschöpfungs-UBI) sind die nach ihrer inländischen Wertschöpfung größten Unternehmen Deutschlands sowie wesentliche Zulieferer für diese Unternehmen.
- UBI 3 (Störfall-UBI) sind Betreiber „eines Betriebsbereichs der oberen Klasse im Sinne der Störfall- Verordnung in der jeweils geltenden Fassung“ oder Betreiber, die, „nach § 1 Absatz 2 der Störfall-Verordnung diesen gleichgestellt sind.“ Für UBI 3 (Störfall-UBI) gilt seit dem 01.11.2021 eine Meldepflicht.

Melden einer Störung

Die Meldung einer IT / OT [7] Störung bei Störfall-UBI (UBI 3) erfolgt an die zentrale Meldestelle des nationalen IT-Lagezentrums im BSI. Für Meldungen von Störfall-UBI (UBI 3) wurde das E-Mail-Postfach meldungen-ubi@bsi.bund.de eingerichtet.

Meldepflichtige IT / OT Störungen sollen unverzüglich gemeldet werden. Hierbei gilt der Grundsatz: Schnelligkeit vor Vollständigkeit. Die Inhalte des Formulars müssen daher bei der ersten Meldung nicht vollständig sein; fehlende Informationen können im Nachgang durch eine weitere Meldung ergänzt werden. Die neue Meldepflicht gegenüber dem BSI entbindet nicht von anderen Meldepflichten gegenüber anderen Behörden.

Unterstützung durch das BSI

Das BSI unterstützt UBI u.a. mit einer Vielzahl an Angeboten, beispielsweise:

- der Allianz für Cyber-Sicherheit (ACS)
- Warnmeldungen (zusätzlich zu den frei verfügbaren Cyber-Sicherheitswarnungen (CSW) auch nach Traffic-Light-Protocol eingestufte CSW)
- Lagebildprodukte, wie den BSI-Monatsbericht zur Cyber-Sicherheitslage
- Cyber-Sicherheitsempfehlungen
- Partnerangebote aus dem Netzwerk der ACS
- Veranstaltungen zu aktuellen Themen der Cyber-Sicherheit
- Austauschformaten wie ERFA- und Expertenkreise
- Weitere Publikationen wie beispielsweise die IT-Notfallkarte

Weiterhin stellt das BSI mit dem IT-Grundschutz relevante Informationen zur Informationssicherheit zur Verfügung.

[7] Operational Technology (OT)

6.4 Zusammenarbeit und Aktivitäten des BSI

Auf Grundlage der im Jahr 2020 zwischen dem BSI und dem KBA geschlossenen Verwaltungsvereinbarung, unterstützt das BSI das KBA bei den Prozessen zur Typgenehmigung nach den UNECE-Regelungen UN-R155 und UN-R156. Im Berichtszeitraum hat das BSI mehrere CSMS- bzw. SUMS-Audits [8] bei Herstellern im Rahmen der Benennung Technischer Dienste (Witnessing) begleitet. Das KBA und das BSI haben ihre Zusammenarbeit auch für den Bereich der Marktüberwachung und den Austausch von Informationen zu IT-bezogenen Vorfällen und Schwachstellen vertieft.

Das KBA hat im Dezember 2021 die weltweit erste Typgenehmigung im Bereich des automatisierten Fahrens für ein automatisches Spurhaltesystem (Automated Lane Keeping System – ALKS) auf Basis der UN-R157 für ein Modell des Herstellers Mercedes-Benz erteilt (16). Dieses System entspricht der Automatisierungsstufe 3 nach der Norm SAE J3016, bei der die Fahrerin oder der Fahrer die automatische Steuerung nicht dauernd überwachen, jedoch stets übernahmebereit sein muss. Voraussetzung für die Genehmigung war u.a. die Erfüllung der Anforderungen zur Cyber-Sicherheit nach der UN-ECE-Regelung UN-R155. Das im Vorfeld durchgeführte Audit des CSMS beim Hersteller, wurde ebenfalls im Rahmen des Witnessings durch das BSI begleitet.

Im Januar 2022 hat das BSI die Technische Richtlinie BSI-TR-03164 „Guidance for Cooperative Intelligent Transport Systems (C-ITS)“ publiziert. In kooperativen, intelligenten Transportsystemen kommunizieren vernetzte Verkehrsteilnehmer und Verkehrsinfrastruktur miteinander. Ziel ist es, auf Basis der ausgetauschten Informationen den Straßenverkehr sicherer, komfortabler und effizienter zu gestalten. Auf europäischer Ebene wurden dafür eine Certificate Policy (CP) und weitere Standards entwickelt. Die Technische Richtlinie ist als Ergänzung zur CP und den einschlägigen Standards zu sehen und dient als Richtlinie für den Betrieb von Public-Key Infrastrukturen und C-ITS Stationen im europäischen Anwendungskontext. Ziel der Technischen Richtlinie BSI TR-03164 ist es, Lücken in den Vorgaben zu schließen und Vorgaben zu konkretisieren, um ein durchgehend hohes und konsistentes Sicherheitsniveau bei allen Instanzen zu ermöglichen und die Interoperabilität der C-ITS Teilnehmer zu gewährleisten.

Die Technische Richtlinie BSI TR-03164 besteht aus zwei Teilen. Der erste Teil, BSI TR-03164-1, dient als Richtlinie für PKI-Betreiber für die Implementierung und den Betrieb von Zertifizierungsstellen innerhalb einer C-ITS PKI. Der zweite Teil, BSI TR-03164-2, dient als Richtlinie für die Konfiguration, Registrierung und den Betrieb von C-ITS Stationen. Beide Teile sind so aufeinander abgestimmt, dass sie in Kombination ihre Wirkung entfalten.

[8] Cyber Security Management System (CSMS), Software Update Management System (SUMS)

7. Chancen und Risiken: Ein Blick in die nahe Zukunft

Im Zuge der Digitalisierung wird sich die elektrische und elektronische Architektur (E/E-Architektur) im Fahrzeug zunehmend ändern. Eine bisherige typische Fahrzeugarchitektur besteht aus einigen Dutzend, bis über hundert einzelnen Steuergeräten (electronic control units, ECU), die über ein Bordnetz miteinander verbunden sind. Diese Steuergeräte kapseln, als eingebettete Systeme, Hard- und Firmware und übernehmen jeweils eine festgelegte Funktion. Das Bordnetz kann dabei in verschiedene Funktionsdomänen eingeteilt sein.

Neue und zukünftige Funktionen, wie etwa das automatisierte Fahren, erfordern eine hohe Rechenleistung zur Auswertung der umfangreichen Sensordaten und zur Umsetzung in die Fahrzeugsteuerung. Dies lässt eine Bündelung der erforderlichen Einzelfunktionen in leistungsfähigen Zentralsteuergeräten sinnvoll erscheinen. Funktionen, die vormals in einzelnen ECUs realisiert wurden, werden durch diese zentralen Einheiten übernommen. Auf diesen kommen vollwertige (Echtzeit-)Betriebssysteme und Softwarestacks zum Einsatz. Verschiedene Funktionsbereiche können beispielsweise durch Virtualisierung voneinander abgegrenzt werden. Vorteil dieser Architektur ist auch die einfachere Möglichkeit, Software-Updates einzuspielen, da die Update-Funktionalität nicht in jedem Steuergerät separat implementiert werden muss. Neue und verbesserte Funktionalitäten, die auf komplexer Software basieren, können so auf einfache Art angeboten werden. Im Fall von Produktionsmängeln können durch die Möglichkeit, Updates über die Luftschnittstelle einzuspielen, unter Umständen aufwändige Rückrufe mit Werkstattbesuchen vermieden werden (17).

Die Erfahrungen aus der klassischen Softwareentwicklung zeigen, dass hier ein engmaschiges Sicherheitsmanagement, sowohl in der Entwicklung, als auch im Feld erforderlich ist, um Sicherheitsrisiken zu minimieren. Regelmäßige Sicherheitsupdates werden zum Normalfall. In der Entwicklung kann die Verwendung moderner Programmiersprachen hilfreich sein, siehe Textkasten „Die Programmiersprache Rust in der Automobilbranche“. Eine besondere Herausforderung sind in dieser Hinsicht die komplexen Software-Lieferketten, die das Auffinden und Beheben von Schwachstellen erschweren können.

Verschiedene Fahrzeughersteller entwickeln derzeit eigene Softwareplattformen für ihre Produkte und tätigen entsprechend umfangreiche Investitionen. Auf der anderen Seite forcieren die großen Technologiekonzerne einen umfassenderen Zugriff Ihrer Produkte (Smartphones) auf das Infotainmentsystem im Fahrzeug, oder sie entwickeln für diesen Zweck eigene im Fahrzeug lauffähige Betriebssystem-Versionen, wie beispielsweise Android Automotive (18).

Die Industrie bleibt hier gefordert, die Cyber-Sicherheit in allen Phasen und unternehmensübergreifend durch geeignete Entwicklungsprozesse zu gewährleisten.

Die Programmiersprache Rust in der Automobilbranche

Die 2010 als Alternative zu C++ ins Leben gerufene Programmiersprache, ursprünglich von Mozilla Research entwickelt, erfährt seit Jahren großen Zuspruch aus der Entwickler-Community. Stackoverflow, eine von technisch Versierten, global weit genutzte Plattform, verkündet zum sechsten Mal in Folge: Rust ist die beliebteste Sprache unter Programmieren und Programmiererinnen (19).

Im April diesen Jahres veröffentlichte nun AUTOSAR, ein Zusammenschluss von Automobilherstellern und Zulieferern zur Standardisierung der Softwarearchitektur für Elektronische Steuergeräte, ein Pressestatement, nach dem der Einsatz von Rust im Kontext von Adaptive Autosar nun aktiv diskutiert wird (20).

Bislang wurde dieser Bereich im Wesentlichen von C++ dominiert. C und C++ sind tief in der Automobilbranche verwurzelt. Die Sprachen sind standardisiert, schon Jahrzehnte in der Nutzung und fußen auf gereiften Ökosystemen. Softwarestandards wie AUTOSAR Classic und AUTOSAR Adaptive setzen auf C und C++. Software Development Guidelines wie MISRA-C und MISRA-C++ unterstützen die Entwicklung sicherheitsrelevanter Systeme. Spezielle, zertifizierte Toolchains wie sie der sechste Teil der ISO 26262, ein etablierter Standard in der Automobilindustrie zur funktionalen Sicherheit, fordert, werden von diversen Zuliefern vertrieben.

Rust hat sehr attraktive Eigenschaften. Genau wie C++ bietet die Sprache ein sehr hohes Maß an Kontrolle für Programmierende, Performanz und ein gleichzeitig hohes Abstraktionsniveau. Die Sprache eignet sich sowohl für die hardwarenahe Programmierung von Embedded Systemen, als auch für die Applikationsentwicklung bei Desktop Systemen. Im Gegensatz zu C++ setzt Rust allerdings ein sehr striktes und mächtiges Typsystem durch, wodurch die Sprache ganze Klassen von Schwachstellen, die mit C und C++ nicht selten zustande kommen, bereits zur Kompilierzeit abfängt. Zu diesen Schwachstellenklassen gehören insbesondere sogenannte „Data Races“ und Speicherzugriffsverletzungen.

Darüber hinaus kommt Rust mit einer modernen Toolchain daher, die beispielsweise auch modernes Fuzzing direkt in den Entwicklungsprozess integriert (21). Eine für die Automobilentwicklung zertifizierte Toolchain, wie für C/C++, existiert bislang jedoch nicht, auch wenn es hier aktive Bemühungen gibt (22).

Literatur-verzeichnis

(1) https://www.bmwk.de/

(2) https://www.theregister.com/2022/02/10/mazda_radios_images/

(3) https://github.com/Hamled/mazda-format-string-bug

(4) https://medium.com/@david_colombo/how-i-got-access-to-25-teslas-around-the-world-by-accident-and-curiosity-8b9ef040a028

(5) https://research.nccgroup.com/2022/05/15/technical-advisory-tesla-ble-phone-as-a-key-passive-entry-vulnerable-to-relay-attacks/

(6) https://www.heise.de/news/Forscher-demonstriert-Tesla-Klau-mit-heimlich-eingeschleustem-Nachschluessel-7133766.html

(7) https://www.bleepingcomputer.com/news/security/honda-bug-lets-a-hacker-unlock-and-start-your-car-via-replay-attack/

(8) https://presse.adac.de/meldungen/adac-ev/technik/keyless-problem-noch-immer-nicht-geloest.html

(9) S. Köhler, R. Baker, M. Strohmeier, I. Martinovic: „Brokenwire: Wireless Disruption of CCS Electric Vehicle Charging“, arXiv preprint, Februar 2022, https://arxiv.org/abs/2202.02104

(10) https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220128_Forschungsprojek-KI-Auto_BSI-ZF.html

(11) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/Allgemeine-Empfehlungen/Empfehlungen-fuer-ICS-Betreiber/empfehlungen-fuer-ics-betreiber.html

(12) https://www.capgemini.com/wp-content/uploads/2021/09/Next-Destination-Software-_WEB-1.pdf

(13) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html

(14) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html

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

https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

(16) https://www.kba.de/DE/Service/Nachrichten/2021/PM/PM_Nr_49_2021_erste_Genehmigung_automatisierten_Fahren.html

(17) https://www2.deloitte.com/cn/en/pages/consumer-business/articles/software-defined-cars-industrial-revolution-on-the-arrow.html

(18) https://source.android.com/devices/automotive/start/what_automotive

(19) https://insights.stackoverflow.com/survey/2021#technology-most-loved-dreaded-and-wanted

(20) https://www.autosar.org/news-events/details/autosar-investigates-how-the-programming-language-rust-could-be-applied-in-adaptive-platform-context/

(21) https://github.com/rust-fuzz/cargo-fuzz

(22) https://ferrous-systems.com/ferrocene/

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582- 0

Kontakt
automotive@bsi.bund.de

Stand
September 2022

Konzept und Gestaltung
Bundesamt für Sicherheit in der Informationstechnik

Druck
Appel und Klinger Druck & Medien GmbH
Bahnhofstraße 3
96277 Schneckenlohe
www.ak-druck-medien.de

Bildnachweis
Titel und Rückseite: AdobeStock © Open Studio, S. 02 und 4: AdobeStock © envfx, Seite 6/7: AdobeStock © sdecoret, S. 8/9: AdobeStock © Open Studio, S. 10: AdobeStock © jamesteohart, Seite 12/13: AdobeStock © metamorworks, S. 16: AdobeStock © Gorodenkoff, S. 19: AdobeStock © Gorodenkoff, S. 20: AdobeStock © metamorworks, S. 26: AdobeStock © SergeyBitos, S. 31: AdobeStock © envfx.

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