Branchen-lagebild Automotive

Cyber-Sicherheit in der Automobilbranche 2022/2023

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Inhalt


00:00:12
a/120
p
b/0
00:01:21
c
00:04:12
ON
ON
LOREM IPSUM
EXE
120
FIX
FIX CAR ERROR
FIX CAR ERROR

1. Einleitung

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

Das vorliegende „Branchenlagebild Automotive“ berichtet in seiner dritten Ausgabe zur IT-Sicherheitslage in der Automobilbranche und im Straßenverkehrsbereich aus Sicht des BSI für den Berichtszeitraum Juli 2022 bis Juni 2023.

Kapitel 2 befasst sich mit den Auswirkungen der Cyber-Kriminalität und von Supply-Chain-Angriffen auf die Unternehmen der Branche. Kapitel 3 beleuchtet IT-Vorfälle mit Bezug zu im Straßenverkehr eingesetzten Produkten und Technologien. Kapitel 4 liefert eine Einschätzung zur IT-Sicherheit der Produktionsanlagen und -prozesse der Branche. In Kapitel 5 werden neue gesetzliche Regelungen und Standardisierungsaktivitäten betrachtet, die die Automobilbranche und den Straßenverkehr betreffen. Schließlich wirft Kapitel 6 einen Blick auf technologische und regulative Entwicklungen, die in den kommenden Jahren von Bedeutung sein werden.

2. 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 Vertragsstaaten maßgeblich sind.

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 Mitgliedsstaaten 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.

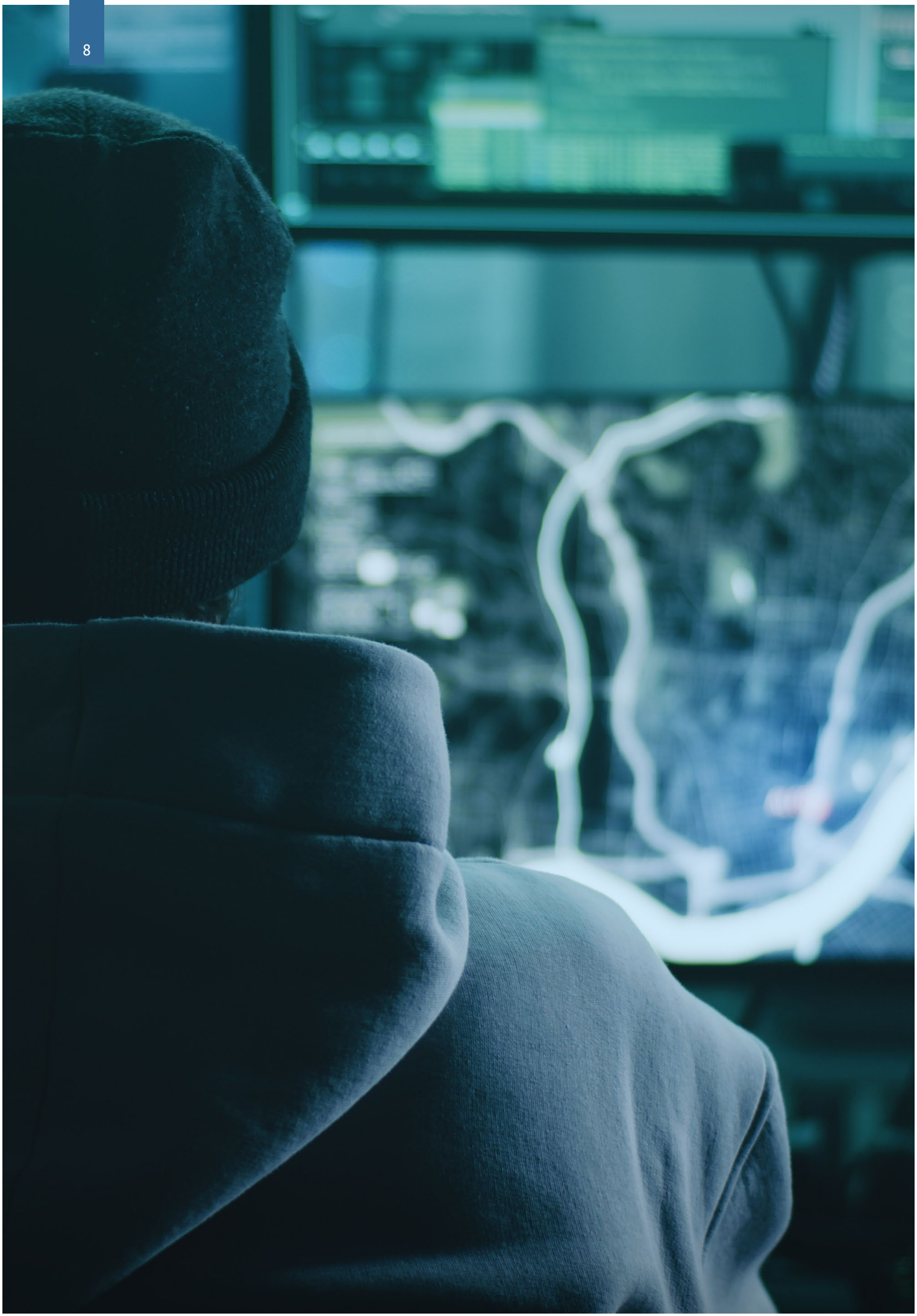
Die Branche setzt sich aus den Automobilherstellern, deren Zulieferern, Entwicklern und sonstigen Dienstleistern zusammen. Es handelt sich um die größte Branche des verarbeitenden Gewerbes und um den Industriezweig mit dem größten Umsatz in Deutschland.

[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.

Branchenüberblick

2022 wurde ein Gesamtumsatz von etwa 506 Mrd. Euro (davon 154 Mrd. Euro im Inland) erzielt. Es waren im Jahresdurchschnitt etwa 774.339 Personen in dieser Industrie beschäftigt. (1)

Der Bestand an Kraftfahrzeugen nimmt in Deutschland weiterhin kontinuierlich zu. Am 1. Januar 2023 waren in Deutschland rund 60,1 Millionen Kraftfahrzeuge zugelassen. Das entspricht einem Anstieg von +1,0 Prozent im Vergleich zum 1. Januar 2022. Im Jahr 2022 wurden insgesamt 3,55 Millionen Kraftfahrzeuge und -anhänger, darunter 2,65 Millionen Personenkraftwagen, erstmals zugelassen. (2)



2.1 Gefahren durch Cybercrime

Die höchste Schadenswirkung geht von cyberkriminellen Angriffen mit Ransomware und Daten-Leaks aus, der sogenannten Double Extortion. Eine Vielzahl der beobachteten Angriffe richtet sich gegen solvente Organisationen und Unternehmen, auch aus der Automobilbranche. Die Angreifer gehen bei der Auswahl ihrer Ziele prinzipiell opportunistisch vor. Ziel der Angreifer ist es, den Betroffenen unter Druck zu setzen, um eine möglichst hohe Lösegeld- und Schweigegeldzahlung durchzusetzen.

Ransomware-Angriffe auf das Büronetzwerk eines Betroffenen wirken sich oftmals unmittelbar auf die Produktion aus, da zum Beispiel Wareneingang und -ausgang oder auch die Rechnungsstellung im Büronetzwerk bearbeitet werden. Somit kommt es zur Beeinträchtigung der Produktion, auch wenn sich der Angriff nicht gegen die Industrial-Control-Systeme (ICS) richtete.

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.

Die Mehrheit der bekannt gewordenen Fälle, in denen Daten veröffentlicht wurden, können den Ransomware-as-a-Services (RaaS) LockBit 3.0, Alphv, Black Basta und Royal zugeordnet werden. Die Angriffe folgen dabei ähnlichen Mustern, unabhängig von der eingesetzten Ransomware.

Am Ende der Ausbreitung im Netzwerk des Betroffenen stehlen die Angreifer Daten zur Veröffentlichung auf der Leak-Seite und spielen die Ransomware auf Windows- und Linux-Systemen sowie Virtualisierungsservern wie ESXi aus.

Maßnahmenempfehlungen

Es können verschiedene Maßnahmen präventiv ergriffen werden, um Ransomware-Angriffe abzuwehren und etwaige Schäden zu minimieren. Hierzu zählt die Absicherung von über das Internet erreichbaren Systemen durch Härtung und Patches sowie Limitierung von Möglichkeiten zur Ausführung von Programmen und Code, welche nicht vorher autorisiert wurden. Innerhalb des Netzwerks können weiterführende Maßnahmen ergriffen werden, wie die Netzwerksegmentierung und die Absicherung von Administratoren-Accounts. Zur Verringerung der Schadenswirkung sollten vom Netz getrennte Backups erstellt werden. Weiterhin gilt es, einen Notfallplan für den Worst Case vorzuhalten und diesen auch zu beproben, um Fallstricke möglichst früh zu erkennen. Das Bundesamt für Sicherheit in der Informationstechnik stellt diese und weitere Maßnahmen auf einer Informationsplattform zum Thema Ransomware zur Verfügung:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Ransomware-Angriffe/ransomware-angriffe_node.html

2.2 Bedeutung der Informationssicherheit in der Supply Chain

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 Kontext des russischen Angriffskriegs gegen die Ukraine bestand eine Bedrohung vor allem durch prorussische Hacktivismus-Angriffe, die aber keinen nachhaltigen Schaden verursachten und eher als Propaganda-Mittel zu werten sind. Im Berichtszeitraum waren einige Vorfälle von Produktionsausfällen oder -störungen bei Zulieferern und IT-Dienstleistern innerhalb der Lieferketten zu beobachten.

Cyber-Angriff auf einen Rüstungs- und Technologiekonzern

In Q1/2023 wurde ein Rüstungs- und Technologiekonzern gleich zweimal Opfer eines Cyber-Angriffs. Ein Unternehmenssprecher bestätigte einen Angriff auf den zivilen Geschäftsbereich des Konzerns. Dieser beliefert industrielle Kunden, hauptsächlich aus dem Automotive-Sektor. Bei dem Angriff soll Ransomware zum Einsatz gekommen sein. Mehreren Medienberichten zufolge sollen auch Tochterunternehmen von dem Angriff betroffen gewesen sein. IT-Systeme waren ausgefallen, die Produktion eingeschränkt, teilweise mussten Mitarbeitende die Arbeit unterbrechen und wurden nach Hause geschickt. Der militärische Geschäftsbereich sei nicht betroffen gewesen.

Offenbar unabhängig von dem finanziell motivierten Ransomware-Vorfall im April erfolgte bereits im März 2023 ein Aufruf von Killnet via

Post-Telegram zu einem „DDoS-Cyber-Angriff“ auf IP-Adressen des Unternehmens. Damals kam es nach Aussage des Unternehmens bis auf eine zeitweise Nichterreichbarkeit der Firmenhomepage zu keinen weiteren Einschränkungen. Unternehmen und Organisationen sollten ein besonderes Augenmerk auf den Schutz gegen diese Art von Angriffen legen. Das BSI hat eine Übersicht zertifizierter DDoS-Mitigations-Dienstleister veröffentlicht.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister-DDos-Mitigation-Liste.html

Supply-Chain-Angriff auf internationalen IT-Sicherheitsdienstleister

In Q1/2023 wurde durch einen internationalen IT-Sicherheitsdienstleister über eine Supply-Chain-Angriffskampagne berichtet, welche auf eine Anwendung für Videokonferenzen und Online-Kommunikation abzielt. Hier wurden verdächtige Aktivitäten bemerkt, welche von einer legitimen und signierten Anwendung stammen. Diese soll unbemerkt Verbindung zu einem C2-Server des Akteurs aufnehmen.

Daraufhin wird ein schadhafter Code geladen und die betroffenen Systeme können aus der Ferne bedient werden. Zum Kundenbereich des internationalen IT-Sicherheitsdienstleisters zählen auch Unternehmen aus dem Automotive-Sektor.

Das Besondere: Der initiale Angriffsvektor zur Kompromittierung der Anwendung liegt in einer eingesetzten, ebenfalls legitim signierten Anwendung, welche ihrerseits kompromittiert wurde und eine Backdoor beinhaltet. Somit handelt es sich um den ersten bekannt gewordenen Fall eines kaskadierten Supply-Chain-Angriffs. Mithilfe der Tarnung als legitime Software ermöglichen es Supply-Chain-Angriffe den Akteuren im Cyber-Raum, innerhalb kurzer Zeit zahlreiche IT-Netze zu kompromittieren.

Ransomware-Angriff auf Automobilzulieferer

In Q2/2022 hatten Angreifer die IT-Systeme eines Automobilzulieferers angegriffen. Diesen Angriff hat das Unternehmen selbst detektiert und daraufhin abwehren können. Die Geschäftsaktivitäten wurden nicht beeinträchtigt. Das Unternehmen hat unmittelbar nach Bekanntwerden des Angriffs alle erforderlichen Abwehrmaßnahmen ergriffen, um die vollumfängliche Integrität der IT-Systeme wiederherzustellen. Zudem wurden die zuständigen (Sicherheits-)Behörden über den Vorfall informiert und standen im engen Austausch mit dem Unternehmen. Ein qualifizierter Incident-Response-Dienstleister wurde vor Ort für eine umfangreiche Analyse der Unternehmensnetzwerke hinzugezogen. Es scheint keine Beeinträchtigung von IT-Systemen Dritter erfolgt zu sein. Das Unternehmen wurde jedoch von der Ransomware-Gruppe LockBit 3.0 auf deren Leak-Seite als mutmaßliches Opfer gelistet. Zudem wurde mit der Veröffentlichung aller angeblich gestohlenen Daten gedroht. Das Unternehmen hatte den Angriff in einer Pressemitteilung öffentlich kommuniziert und über die erfolgreiche Abwehr berichtet.

Bei einer Supply-Chain-Attacke wird nicht direkt das eigentliche Ziel angegriffen, sondern ein schwächer geschütztes Element in der Versorgungskette. Durch die Kompromittierung des schwächer geschützten Elements kann nun das eigentliche Ziel angegriffen werden. Die Digitalisierung und Stärkung der Liefernetzwerke sind zentrale Herausforderungen und zugleich die Chancen der Automobilwirtschaft in Deutschland. Voraussetzung hierfür ist jedoch, die Informationssicherheit in der Supply Chain sicherzustellen sowie diese resilienter zu machen.

3 Cyber-Sicherheit im Straßen-verkehr

Die Cyber-Sicherheit ist eine wesentliche Voraussetzung für die weitere Digitalisierung im Straßenverkehr. Hersteller sind gemäß Vorgaben für die Typgenehmigung verpflichtet, die Cyber-Sicherheit in der Entwicklung zu berücksichtigen und die Sicherheitslage für ihre Produkte fortlaufend zu beobachten.

Auch im zurückliegenden Berichtszeitraum sind einige IT-Sicherheitsprobleme, die Fahrzeuge bzw. die Straßenverkehrsinfrastruktur betreffen, bekannt geworden.

3.1 Vernetztes Fahren

Fahrzeugdiebstahl

Im Branchenlagebild Automotive 2021/2022 wurde bereits von der verbreiteten Ausnutzung von Sicherheitslücken für die Durchführung von Autodiebstählen bzw. das unbefugte Öffnen von Fahrzeugen berichtet. Dieses Problem besteht auch in diesem Berichtszeitraum unvermindert fort. In den folgenden Abschnitten werden drei Arten genauer vorgestellt.

Unzureichende Rollcodes

Die Schließsysteme von Fahrzeugen (die über Funkschlüssel bedient werden) sind durch sogenannte Rollcodes (Rolling Codes) geschützt. Nach der UNECE-Regelung 116, die einheitliche technische Vorschriften für den Schutz von Kraftfahrzeugen gegen unbefugte Benutzung enthält, ist ein Rollcode ein „elektronischer Code, der sich aus mehreren Elementen zusammensetzt, deren

Kombination sich nach jeder Betätigung der Übertragungseinheit nach dem Zufallsprinzip ändert“. Rollcodes können etwa über einen Pseudo-Zufallszahlengenerator implementiert sein, wobei die Zufallszahlen aus einem gemeinsamen Geheimnis von Funkschlüssel und Schließsystem im Auto und einem Zustandszähler abgeleitet werden. Rollcodes bieten einen einfachen Schutz gegen Replay-Attacken. Ein etwa durch einen Angreifer aufgezeichnetes Signal des Funkschlüssels zum Öffnen des Fahrzeugs kann nicht wiederverwendet werden, da der Zustandszähler hochgezählt wird und das Fahrzeug für den nächsten Öffnungsvorgang einen anderen Zufallswert erwartet.

Der beschriebene Schutz lässt sich je nach Modell auf verschiedene Arten umgehen. Ein prominentes Beispiel ist der RollJam-Angriff (3), bei dem zwei aufeinanderfolgende Signale des Funkschlüssels aufgezeichnet werden, wobei gleichzeitig die Übertragung an das Fahrzeug per Funkstörung geblockt wird, so dass diese Signale später als noch „nicht verbraucht“ gelten. Werden diese Signale in geeigneter Art und Weise durch den Angreifer wieder eingespielt, kann dieser so unbefugt das Fahrzeug öffnen.

Bei den im Juli und August 2022 veröffentlichten Rolling-Pwn- und RollBack-Angriffen (4) (5) kann durch Wiedereinspielen vorher aufgezeichneter Schlüsselsignale in manchen Implementierungen sogar der Zustandszähler im Fahrzeug wieder zurückgesetzt werden. Auf diese Weise kann (im Gegensatz zum RollJam-Angriff) das Fahrzeug beliebig oft zu beliebigen Zeiten geöffnet werden.

Die Beispiele zeigen, dass einfache Rollcodes für einen wirksamen Schutz nicht ausreichen. Hersteller müssen die Schließsysteme (und Wegfahrsperren) mit zusätzlichen kryptographischen Mechanismen sichern, um derartige Angriffe zu verhindern.

CAN-Injection

Die Bemühungen der Fahrzeughersteller, die bekannten Schwachstellen zu beheben, führen auch dazu, dass Fahrzeugdiebe versuchen, andere Schwachstellen auszunutzen, um Erfolg zu haben. Im April 2023 hat Dr. Ken Tindell, Chief Technology Officer von Canis Automotive Labs, in seinem Blog von der Methode CAN-Injection berichtet (6). Bei dieser Methode verschafft sich der Angreifer physischen Zugriff auf den CAN-Bus, an dem die ECU für die Validierung des Schlüsselsignals (Schließsystem-ECU) hängt. Im dort beschriebenen Fahrzeugmodell war auch das Abblendlicht an den Bus angeschlossen. Das Abblendlicht wurde mit geringem Aufwand entfernt, und so hatte der Dieb Zugriff auf den entsprechenden CAN-Bus. Mit Hilfe eines sogenannten CAN-Injectors ist es dann möglich, die gleichen CAN-Nachrichten auf den CAN-Bus zu senden, die normalerweise die Schließsystem-ECU nach erfolgreicher Validierung sendet. Da keine weitere kryptographische Prüfung über die Herkunft der Nachricht durchgeführt wird, wird die Nachricht von den entsprechenden ECUs akzeptiert, so dass die Türen entriegelt werden oder der Motor startet. Die dafür benötigten CAN-Injectors können entweder mit einfachen CAN-Komponenten selbst gebaut werden oder für einige tausend Euro in entsprechenden Onlineshops gekauft werden, die dann Angriffe auf unterschiedliche Marken erlauben. Der von Tindell untersuchte CAN-Injector war in einem tragbaren Lautsprecher eingebaut, um unauffällig transportiert werden zu können und keinen Verdacht zu erregen bei einer möglichen Verkehrskontrolle.

Die von Tindell beschriebene Untersuchung wurde nur an einem Fahrzeugmodell durchgeführt. Es ist jedoch damit zu rechnen, dass viele der Fahrzeugtypen mit dieser Methode entwendet werden können. Die betroffenen Fahrzeughersteller sollten möglichst schnell Updates liefern, um diese Methode effektiv zu verhindern.

Web- und API-Schwachstellen im Automobilbereich

Eine Gruppe um den Sicherheitsforscher Sam Curry hat Ende 2022 nach Schwachstellen in den APIs von Telematik-ECUs von Fahrzeugen verschiedener Hersteller gesucht. Das Ziel dabei war es unter anderem, die Fahrzeuge aus der Ferne zu öffnen, zu starten oder zu orten.

Die gefundenen Schwachstellen wurden Anfang Januar 2023 auf dem Blog des Sicherheitsforschers veröffentlicht (7). Zu diesem Zeitpunkt waren bereits alle Hersteller der betroffenen Fahrzeuge und Dienste informiert worden und es war sichergestellt, dass die Schwachstellen behoben sind.

Die gefundenen Schwachstellen lassen sich in mehrere Kategorien unterteilen:

1. Zugriff auf Entwicklungs- und Administrations-Plattformen von Fahrzeugherstellern und -händlern: Bei einem Hersteller war es möglich, über die Passwort-zurücksetzen-Funktion und das Umgehen der Zwei-Faktor-Authentisierung Zugriff auf die Händlerportale zu erhalten. Bei einem anderen Hersteller war es möglich, mit Hilfe eines auf einer Website für Werkstätten angelegten Accounts auch Source Code Repositories und andere Entwicklungsdienste eigentlich unabhängiger Plattformen des gleichen Herstellers zu nutzen.

2. Zugriff auf Fahrzeugfunktionen über Smartphone-Apps: Viele moderne Fahrzeuge erlauben das Öffnen, Orten oder Starten des Fahrzeugs über Hersteller-Apps. Die Sicherheitsforscher konnten bei einem Hersteller nur mit Kenntnis der Fahrzeugidentifikationsnummer (VIN) Zugriff auf verschiedene Fahrzeugfunktionen über die Fahrzeug-App erhalten. Die VIN ist oftmals von außen sichtbar hinter der Windschutzscheibe angebracht. Eine weitere Authentisierung war nicht notwendig. Bei einem anderen Fahrzeughersteller war es möglich, die Überprüfung der E-Mail-Adresse im JSON Web Token durch das Anhängen eines CRLF (Carriage Return/Line Feed) an die E-Mail-Adresse zu umgehen und so ebenfalls Zugriff auf den Account zu erhalten, um das Fahrzeug zu öffnen und zu starten.

3. Übernahme von Nutzerkonten: Eine weitere Schwachstelle war die Übernahme von Nutzerkonten durch SQL-Injection auf der Website eines Anbieters. Hierbei war es möglich, alle Nutzerdaten und Fahrzeugpositionen einzusehen.

Die Untersuchungen zeigen, dass Fahrzeugfunktionen vermehrt durch die Nutzung von Nutzerkonten gesteuert und überwacht werden können. Die Fahrzeughersteller und Diensteanbieter haben dafür zu sorgen, dass die Nutzerkonten entsprechend dem Stand der Technik abgesichert sind, so dass die Integrität der Konten gewährleistet ist und der Zugriff auf die Fahrzeugfunktionen und -daten den legitimen Nutzern vorbehalten ist.

SQL-Injection

Mit Hilfe der Datenbanksprache SQL werden Datensätze aus Datenbanken gelesen oder verändert.

Bei der SQL-Injection versuchen Angreifer, einen eigenen SQL-Code z. B. in Eingabemasken von Webseiten einzuschleusen, um beispielsweise vertrauliche Informationen wie Nutzerdaten abzugreifen oder geschützte Daten wie Nutzerrechte unerlaubt zu ändern.

SQL-Injection ist meist auf mangelnde Validierung von Eingaben zurückzuführen und wird auch von der Open Worldwide Application Security Project (OWASP) zu den 10 größten Risiken für Web-Anwendungen gezählt (8).

3.2 Cyber-Sicherheit beim elektrischen Laden

Die Verbreitung von Elektrofahrzeugen hängt wesentlich von einem zuverlässigen Netz von Ladestationen ab. Da Ladestationen und ihre unterstützende Infrastruktur potenziellen Zugriff auf eine große Anzahl von Fahrzeugen haben, ist die Cyber-Sicherheit dieser Einrichtungen von großer Bedeutung, um mögliche Angriffe auf Elektrofahrzeuge und lokale Stromnetze zu verhindern. Erste Vorfälle im Zusammenhang mit Ladestationen wurden 2018 veröffentlicht. Seit 2020 werden zunehmend Machbarkeitsnachweise (Proof-of-Concepts) bekannt, bei denen Ladestationen kompromittiert wurden. Zeitgleich steigt die Anzahl an veröffentlichten Schwachstellen (CVEs) aus diesem Bereich an. Es wird erwartet, dass dieser Trend anhält und sich in der anstehenden Wachstumsphase der Elektromobilität verstärkt.

Angriffsflächen beim Ladevorgang

Beim Ladevorgang wird das Fahrzeug physisch an die Ladestation angeschlossen. Hierbei wird neben der konduktiven Verbindung zwischen Stromnetz und Batterie auch eine Vielzahl an Kommunikationsverbindungen aufgebaut. Der Ladevorgang zwischen Fahrzeug und Ladestation wird im besten Fall durch Verfahren wie beispielsweise das ISO-15118-Protokoll und TLS-Zertifikate gesichert. Zu den potenziellen Bedrohungen in dieser Phase gehören Angriffe, die Schwachstellen im Kommunikationsprotokoll oder den genannten Sicherheitsmechanismen ausnutzen.

Bei Start des Ladevorgangs erfolgt eine Authentifizierung der Nutzenden des Fahrzeugs. Diese kann u. a. durch eine RFID-Karte, eine Smartphone-App oder eine Kreditkarte, gegebenenfalls in Verbindung mit einer PIN-Eingabe, erfolgen. Zu den potenziellen Bedrohungen in dieser Phase zählen Angriffe, bei denen versucht wird, an Anmeldeinformationen und persönliche Daten wie die Kartendaten oder die PIN zu gelangen. Hierbei könnten auch Schwachstellen oder Fehlkonfigurationen in einem der für die Authentifizierung verwendeten Tools von Drittanbietern ausgenutzt werden.

Der Authentifizierungsprozess gegenüber den Backend-Systemen des Ladedienstanbieters wird vom Managementsystem der Ladestation (CSMS – Charging Station Management System) abgewickelt. Die Kommunikation zwischen der Ladestation im Feld und dem CSMS im Backend erfolgt in der Regel über einen spezifischen Kommunikationsstandard (OCPP – Open Charge Point Protocol). Zu den potenziellen Bedrohungen in dieser Phase gehören serverseitige Angriffe wie XSS (Cross-Site-Scripting) und SQL-Injection-Angriffe, sowie die Verwendung von Anmeldeinformationen, welche aus Quellen Dritter geleakt wurden.

Nach der Anmeldung des Fahrzeugs an der Ladestation erfolgt der Abrechnungsprozess beispielsweise mithilfe eines Kreditkarten-Verifizierungsprozesses. Potenzielle Bedrohungen auf dieser Stufe sind Kreditkartenbetrug, Manipulation von Abrechnungsdaten sowie wiederum der Missbrauch von Schwachstellen im Kreditkartenzahlungssystem, wie z. B. einem unsicheren Zahlungsgateway oder einer schwachen Verschlüsselung.

Bei einem unsicheren Update-Mechanismus kann eine Ladestation auch durch die Installation einer manipulierten Firmware kompromittiert werden. Dies kann unter Umständen zu falschen Betriebsparametern führen und die Ladestation somit unbrauchbar machen oder die Komponenten der Ladestation beschädigen.

Alle diese Angriffsarten zeigen, wie wichtig es ist, die vollständigen Kommunikationsketten in beide Richtungen zu schützen, um potenzielle Risiken zu mindern und vor unbefugtem Zugriff zu schützen. Aufgrund der potenziell großen Anzahl an betroffenen Stationen und Fahrzeugen sowie der möglichen Beeinflussung der elektrischen Infrastruktur bergen Angriffe auf das OCPP das größte Schadenspotenzial. Neben den spezifischen Bedrohungen für Ladestationen kann das CSMS dabei von klassischen IT-Sicherheitslücken betroffen sein. Beispielsweise erfordert OCPP eine TLS-Validierung. Falls ein Angreifer die genaue TLS-Implementierung kennt, die für die Verbindung zwischen der Ladestation und dem CSMS gewählt wurde, und diese eine bekannte Schwachstelle aufweist, die aus der Ferne ausgenutzt werden kann, könnte ein Angreifer den Datenverkehr beeinflussen.

Aus der Praxis wurden in der jüngeren Vergangenheit einzelne Cyber-Vorfälle mit lokalen Auswirkungen auf Ladestationen öffentlich bekannt. Diese Angriffe wurden durch anfällige und/oder zugängliche Komponenten bzw. Software der Ladestation verursacht. Im vergangenen Jahr gab es etwa Meldungen über einen Angriff auf Ladestationen in Russland, der zu einer lokalen Abschaltung der Stationen und einer Manipulation der Displays führte (9). Einen ähnlichen Fall aus dem letzten Jahr stellt ein Hackerangriff auf Ladestationen auf der britischen Isle of Wight dar. Die Stationen wurden von einem Unbekannten gehackt und zeigten nicht jugendfreie Inhalte auf den Bildschirmen (10). Ein weiteres, aktuelles Beispiel ist ein demonstrierter Angriff auf Ladestationen eines Anbieters in den USA im Januar 2023, der zu einer Übernahme des Systems führte. Der Angriff basierte auf dem Missbrauch der installierten Fernwartungssoftware und erlaubte es, die Kontrolle über die Station und deren Anzeige zu übernehmen (11). Angreifer könnten dieses Szenario nutzen, um eine gefälschtes Nutzerinterface zu erstellen und so persönliche Daten von Nutzenden zu stehlen.

Prävention

Es sollten bewährte Maßnahmen zur Cyber-Sicherheit beim Aufbau der Infrastruktur umgesetzt werden. Dazu gehören die Implementierung standardisierter Kommunikationsprotokolle, Verschlüsselungsverfahren und Authentifizierungsmechanismen im gesamten Ökosystem der Elektromobilität und ein wirksames Schwachstellenmanagement, bei dem die Hersteller proaktiv nach neu veröffentlichten Schwachstellen suchen und Patches bereitstellen. Dies beinhaltet auch den Einsatz von Systemen zur kontinuierlichen Überwachung der Ladeeinrichtungen, um potenzielle Cyber-Bedrohungen in Echtzeit zu erkennen und darauf reagieren zu können. Ebenfalls wichtig für diese Zwecke ist der Informationsaustausch zwischen Herstellern und Betreibern von Ladestationen sowie Cyber-Sicherheitsexperten.

3.3 Verkehrsinfrastruktur

In zukünftigen kooperativen intelligenten Transportsystemen bildet die Verkehrsinfrastruktur einen wesentlichen Bestandteil. Einrichtungen wie vernetzte Ampelanlagen, Leitsysteme oder Baustellenwarneinheiten können drahtlos Zustandsinformationen an entsprechend ausgestattete Verkehrsteilnehmer in der Umgebung versenden.

Die bereits bestehende Infrastruktur ist bisher allerdings sehr eingeschränkt für konkrete Einsatzfälle drahtlos vernetzt. Bei diesen teilweise schon vor vielen Jahren installierten Systemen wurden Cyber-Sicherheitsbetrachtungen häufig nicht durchgeführt.

Im Dezember 2022 berichteten das Computermagazin c't, der NDR und der BR über die Anfälligkeit von Ampelsteuerungssystemen für unbefugte Eingriffe. Die sogenannte Lichtsignalanlagen-Beeinflussung wird genutzt, um ÖPNV-Fahrzeugen im Straßenverkehr Vorrang an Ampeln geben zu können. Busse können auf reservierten Betriebsfrequenzbereichen bei Annäherung Nachrichten („R09-Telegramme") an Ampelanlagen senden, die dann in der Fahrtrichtung des Busses vorzeitig auf Grün schalten. Nachdem der Bus die Kreuzung durchfahren hat, sendet er eine Abmeldenachricht an die Ampel, die dann wieder in den ursprünglichen Schaltmodus zurückkehrt.

Das Verfahren wurde in den 80er-Jahren vom Verband der öffentlichen Verkehrsbetriebe (VÖV) spezifiziert. Es wird in vielen Kommunen heute immer noch eingesetzt. Die R09-Telegramme sind kryptographisch nicht geschützt, sind also nicht etwa mit digitalen Signaturen oder Authentisierungs-Codes ausgestattet. Da die VÖV-Schrift öffentlich verfügbar ist, können die Telegramme daher leicht durch Dritte nachgebildet werden. Die Kosten für die notwendige Hardware zum Versenden der Telegramme (wie etwa ein Raspberry Pi und ein Software Defined Radio) bewegen sich im niedrigen dreistelligen Bereich. Um eine bestimmte Ampelanlage zu beeinflussen, ist lediglich die Kenntnis des jeweiligen Meldepunktes (ähnlich einer ID für die Ampel und die Fahrtrichtung) notwendig. Auf diese Weise können z. B. Sabotageakte (massive Störung des Verkehrs in der Hauptverkehrszeit) durchgeführt werden.

Abhilfe können moderne Digitalfunktechnologien schaffen. Beispielsweise können auf kooperativen intelligenten Transportsystemen (C-ITS) basierende Verfahren genutzt werden. Hier wurden bereits entsprechende Dienste („Traffic Light Control Service") und Nachrichtenformate spezifiziert (12), die eine Vorrangschaltung beispielsweise für Einsatzfahrzeuge oder Busse an Ampeln ermöglichen. Das System wird derzeit in Pilotprojekten getestet (13). Die Funknachrichten in C-ITS sind durch digitale Signaturen geschützt, so dass ein einfacher Angriff wie oben beschrieben nicht möglich ist. Dem C-ITS-System liegt eine entsprechende Sicherheitsinfrastruktur (Public-Key-Infrastruktur) zugrunde, die die notwendigen Signatur-Zertifikate verwaltet. Weitere Informationen zur IT-Sicherheit im Bereich intelligenter Verkehrssysteme finden sich unter:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Automotive/Kooperative_Intelligente_Verkehrssysteme/Kooperative_Intelligente_Verkehrssysteme_node.html.

4 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 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.

4.1 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.

Der Trend zu professioneller agierenden Angreifern setzt sich wie in den letzten Jahren fort. Dabei richten sich Angriffe meist weiterhin gegen die Unternehmens-IT. Die Produktion und die Produktionsanlagen sind weiterhin meist nicht direktes Ziel von Angriffen und nur indirekt durch beeinträchtigte Office-Systeme und damit fehlende Auftrags- bzw. Produktionsdaten beeinträchtigt. Trotzdem muss der Schutz der Produktionssysteme weiter forciert werden, um ein entsprechen-

des Informationssicherheitsmanagement zu etablieren. Es gilt, die bestehenden Defizite, insbesondere beim Einsatz von Altsystemen, zu beseitigen, um direkte Angriffe zu verhindern und um Angreifern die Möglichkeit zu nehmen, vorhandene Schwachstellen in den Produktionsanlagen auszunutzen. Dabei stehen sowohl Systeme, die unmittelbar mit dem Internet verbunden sind, als auch diejenigen, welche über Fernzugriffe durch Dienstleister erreicht werden können, im Fokus.

Dies wird zudem durch die zusätzlichen Anforderungen und Verpflichtungen aus der NIS-2-Richtlinie unterstrichen (siehe dazu Kapitel 5.2 „Neuregelungen für Unternehmen nach der NIS-2-Richtlinie“).

Dies spiegelt sich auch in den im Frühjahr 2022 aktualisierten „ICS TOP 10 Bedrohungen und Gegenmaßnahmen“ wider.

4.2 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 der Nutzer 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 Forderung des BSI, zur Verbesserung der Softwarequalität und damit einhergehender Prozesse zum Umgang mit Meldungen über Schwachstellen in ihren IT-Produkten und Systemen einen sogenannten Coordinated-Vulnerability-Disclosure(CVD)-Prozess zu etablieren, werden zunehmend aufgegriffen. Gleiches gilt für die vom BSI aktiv unterstützten Konzepte wie beispielsweise Software Bill of Materials (SBOM) und Common Security Advisory Framework (CSAF).

https://www.bsi.bund.de/csaf

Seit letztem Jahr beginnen erste Hersteller, Informationen entsprechend bereitzustellen. Damit ist eine Voraussetzung geschaffen, dass auch Betreiber diese Automatisierung für das Schwachstellenmanagement in den Produktionsanlagen nutzen können.

4.3 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, zur Wartung und zum Service für Produktionssysteme handeln. Diese müssen 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.

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. Der IT-Grundschutz bietet mit dem Baustein „IND Fernwartung in Produktionsumgebungen“ eine Grundlage. Darüber hinaus hat sich der C5-Standard des BSI, insbesondere bei Cloud-Anbietern, weiter etabliert und kann ebenfalls genutzt werden.

5 Maßnahmen und Aktivitäten

5.1 Regulierung und Standardisierung zur Cyber-Sicherheit im Verkehrsbereich

Die regulativen Vorgaben zur Cyber-Sicherheit in Kraftfahrzeugen gemäß der UNECE-Regelung 155 und der EU-Verordnung 2018/858 müssen seit Juli 2022 von den Herstellern verpflichtend umgesetzt werden. Zahlreiche Hersteller haben entsprechende Audits bereits durchlaufen und verfügen über zur Regelung konforme Cyber-Security-Management-Systeme (CSMS). Ein vorhandenes CSMS bildet die Voraussetzung für die Genehmigung neuer Fahrzeugtypen.

Parallel zur genannten Regelung sind internationale Standards und Spezifikationen entwickelt worden, die Unternehmen der Automobilbranche bei der Umsetzung unterstützen können, etwa der Standard ISO/SAE 21434 „Road Vehicles – Cybersecurity Engineering“ (14) oder die Spezifikation ISO/PAS 5112:2022 „Road Vehicles – Guidelines for auditing cybersecurity engineering“ (15). Die Umsetzung der ISO/SAE 21434 ist aber weder formale Voraussetzung für die Erfüllung der UNECE-Regelung 155, noch ist der Standard deckungsgleich mit den Anforderungen der Regulierung.

Im Mai 2022 hat der Bundesrat die Verordnung zur Regelung des Betriebs von Kraftfahrzeugen mit automatisierter und autonomer Fahrfunktion und zur Änderung straßenverkehrsrechtlicher Vorschriften gebilligt. Diese Verordnung ergänzt das Gesetz zum autonomen Fahren, welches im Juli 2021 in Kraft getreten ist, und regelt u. a. das Verfahren für die Erteilung einer Betriebserlaubnis für entsprechende Kraftfahrzeuge. Der Hersteller ist nach Verordnung verpflichtet, die Anforderungen der UNECE-Regelung 155 zu erfüllen und insbesondere die notwendigen Funkverbindungen der Fahrzeuge zu den Hintergrundsystemen nach Stand der Technik abzusichern. Das Gesetz und die Verordnung ermöglichen auch die Erprobung von automatisierten und autonomen Fahrfunktionen im Straßenverkehr nach Genehmigung durch das Kraftfahrt-Bundesamt (KBA). Das BSI wird an den Erprobungsgenehmigungen beteiligt.

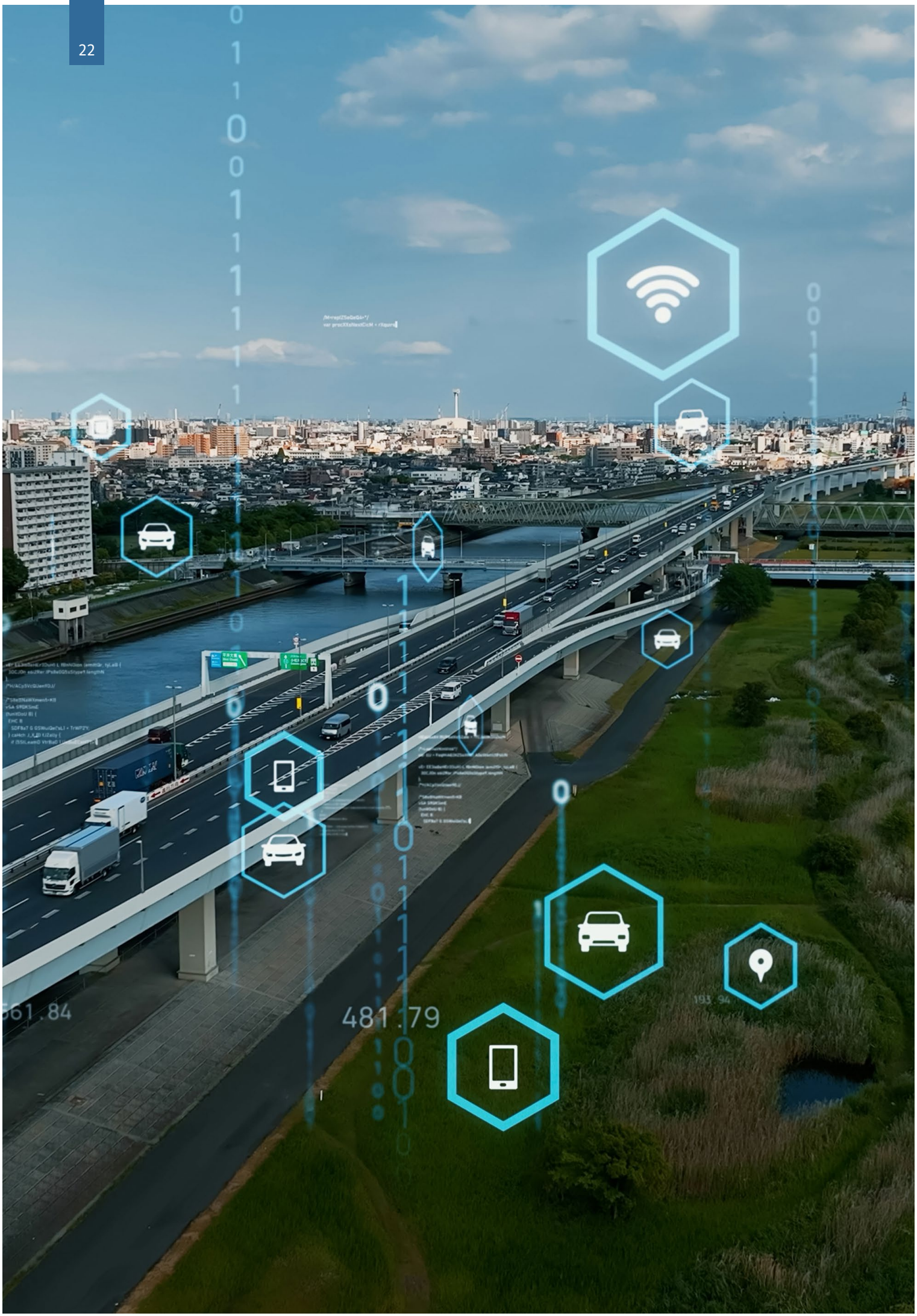
Einen speziellen Anwendungsfall des autonomen Fahrens stellt das Automated Valet Parking (AVP) dar. Bei diesem ist es möglich, die Parkplatzsuche in einem Parkhaus automatisiert ausführen zu lassen. Das Fahrzeug wird dazu an einem Übergabestandort („Drop-off-Zone“) abgestellt. Nach Aktivierung des AVP fährt das Fahrzeug selbstständig auf einen freien Stellplatz im Parkhaus und nach Ende des Parkens auch wieder zurück zu einem Abholbereich. Es werden unterschiedliche Typen des AVP unterschieden, je nachdem, ob das Fahrzeug durch per Funk übertragene Befehle einer mit Sensoren und Kameras ausgestatteten Parkhaus-Infrastruktur gesteuert wird (Typ 2) oder im Wesentlichen eigenständig durch das Parkhaus manövrieren kann (Typ 1).

In Deutschland können Fahrzeuge mit AVP-Systemen als KFZ mit autonomer Fahrfunktion in festgelegten Betriebsbereichen ebenfalls nach dem Gesetz zum autonomen Fahren genehmigt werden. Das KBA hat eine erste Betriebserlaubnis

für ein solches System (vom Typ 2), das zunächst in einem entsprechend ausgerüsteten Parkhaus in Stuttgart verwendet werden kann, im November 2022 genehmigt (16).

Wie im allgemeinen Fall des automatisierten und autonomen Fahrens muss auch in AVP-Systemen die Cyber-Sicherheit betrachtet werden, insbesondere bei Systemen vom Typ 2, bei denen das Fahrzeug auf per Funk übertragende Steuerbefehle reagiert. Möglichen Bedrohungen muss daher mit wirksamen Maßnahmen sowohl im Fahrzeug selbst als auch in der eventuell notwendigen AVP-Infrastruktur begegnet werden. Im Anforderungskatalog für (nachträglich aktivierte) AVP-Systeme, der im Oktober 2022 vom KBA veröffentlicht wurde (17), sind daher explizit Anforderungen bezüglich der Cyber-Sicherheit formuliert. Im Wesentlichen finden die Anforderungen der UNECE-Regelung 155 Anwendung und werden auf die AVP-Infrastruktur erweitert. Im Speziellen ist auch in der Betriebsphase fortlaufend zu beurteilen, ob Gefährdungen und Schwachstellen in Bezug auf die Cyber-Sicherheit vorliegen. Die Möglichkeit der Umsetzung von Schutzmaßnahmen im Nutzungszeitraum, z. B. durch Software-Updates, muss gegeben sein.

Auf Ebene der ISO finden derzeit ebenfalls Standardisierungsaktivitäten zum AVP statt. Der ISO/FDIS 23374-1 (18) wird derzeit um weitere Teile ergänzt, die sich mit der IT-Sicherheit bzgl. der Schnittstellen in den verschiedenen Typen von AVP-Systemen auseinandersetzen (19).


481.79

5.2 Neuregelungen für Unternehmen nach der NIS-2-Richtlinie

Auswirkungen auf die Automobilbranche hat auch die sogenannte NIS-2-Richtlinie der EU (20).

Bei der NIS-2-Richtlinie handelt es sich um die Fortschreibung der NIS-Richtlinie ((EU) 2016/1148), die 2016 in Kraft getreten ist. Die damalige Richtlinie war die erste EU-weite Rechtsvorschrift zur Cyber-Sicherheit mit dem Ziel, ein gleichmäßig hohes Sicherheitsniveau von Netz- und Informationssystemen zu erreichen. Sie richtete sich in erster Linie an Betreiber wesentlicher Dienste (KRITIS-Betreiber) und Anbieter digitaler Dienste, denen Verpflichtungen in den Bereichen Risikomanagement und Meldungen von Sicherheitsvorfällen auferlegt wurden.

Die NIS-2-Richtlinie verpflichtet die Mitgliedsstaaten u. a. zur Festlegung jeweils einer nationalen Cyber-Sicherheitsstrategie und zur Benennung einer zuständigen Behörde und eines Computer Security Incident Response Teams (CSIRT). In Deutschland werden diese beiden Rollen bereits durch das BSI wahrgenommen.

Die CSIRTs sollen u. a. als zentrale Anlaufstelle für eine koordinierte Offenlegung von Schwachstellen (Coordinated Vulnerability Disclosure, CVD) benannt werden. Sie tauschen untereinander relevante Informationen im Rahmen eines CSIRTs-Netzwerks aus. Die ENISA wird verpflichtet, eine europäische Schwachstellendatenbank aufzubauen, die allen interessierten Parteien offenstehen soll.

Der Kreis der betroffenen Unternehmen wird deutlich ausgeweitet. Neben den sogenannten „wesentlichen Einrichtungen", unter die u. a. KRITIS-Unternehmen fallen, werden sog. „wichtige Einrichtungen" aus unterschiedlichen Branchen definiert. Wesentliche und wichtige Einrichtungen unterliegen Meldepflichten für Sicherheitsvorfälle, die signifikante Auswirkungen auf die Leistungserbringung haben. Für die Meldungen werden abgestufte Fristen festgelegt. Meldestelle ist wiederum das jeweilige CSIRT oder die zuständige Behörde. Umgekehrt hat die meldende Entität Anspruch auf ein Feedback mit Hinweisen zum Umgang mit dem Vorfall und möglichen Gegenmaßnahmen.

Typ und Format der Meldungen können durch die EU-Kommission durch Implementierungsrechtsakte festgelegt werden.

Die NIS-2-Richtlinie wurde im November 2022 vom Rat der EU angenommen und im Dezember 2022 im Amtsblatt der Europäischen Union veröffentlicht. Sie muss nun durch die einzelnen Mitgliedsstaaten innerhalb von 21 Monaten nach Inkrafttreten in nationales Recht überführt werden.

Nach Anhang II der Richtlinie werden Hersteller von Kraftwagen und Kraftwagenteilen explizit als „wichtige Einrichtungen" eingestuft. Wie bereits in der NIS-Richtlinie bleiben für Verkehrsmanagement und -steuerung verantwortliche Straßenbetreiber nach Delegierter Verordnung (EU) 2015/962 und Betreiber intelligenter Verkehrssysteme nach Richtlinie 2010/40/EU „wesentliche Einrichtungen".

5.3 Zusammenarbeit und Aktivitäten des BSI

Auf Grundlage der im Jahr 2020 zwischen dem BSI und dem KBA geschlossenen Verwaltungsvereinbarung unterstützt das BSI das KBA weiterhin bei den Prozessen zur Typgenehmigung nach den UNECE-Regelungen 155 und 156. Im Berichtszeitraum hat das BSI CSMS- bzw. SUMS-Audits bei Herstellern im Rahmen der Benennung Technischer Dienste (Witnessing) begleitet. Des Weiteren beteiligt das KBA das BSI gemäß § 1i des Straßenverkehrsgesetzes (StVG) im Rahmen der Erteilung von Genehmigungen für Fahrzeuge zur Erprobung von Entwicklungsstufen von automatisierten oder autonomen Fahrfunktionen bei der Erstellung und Umsetzung sowie bei der Weiterentwicklung und Bewertung technischer Anforderungen.

Im Bereich der Marktüberwachung führt das BSI fortlaufend Bewertungen zu IT-bezogenen Vorfällen und Schwachstellenmeldungen für das KBA durch.

Im März 2023 wurde im Rahmen der Allianz für Cyber-Sicherheit (ACS) der Expertenkreis Automotive CSMS-Audit und Produktprüfung gegründet. Dieser steht anerkannten Auditorinnen und Auditoren, Technischen Diensten sowie Behörden offen und soll als Austauschplattform zur Diskussion von verschiedenen Prüf- und Auditmethoden zur Anwendung in Verfahren basierend auf der UNECE-Regelung 155 dienen. Hierbei findet auch ein Austausch zu technischen Aspekten der Bedrohungslage im Bereich Automotive statt. Es sollen wiederkehrende und typische Auffälligkeiten oder systematische Probleme auf generischer Ebene besprochen werden. Zudem soll eine offene Diskussion über die Landschaft der relevanten internationalen Standards stattfinden. Der Expertenkreis wird künftig zweimal im Jahr tagen.

https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Netzwerk-Formate/Veranstaltungen-und-Austausch/Expertenkreise/automotive/automotive_node.html

Das BSI arbeitete zusammen mit einem externen Auftragnehmer zwischen 2021 und 2023 an einem Projekt zu Hard- und Softwareanalysen von vernetzten Fahrzeugen, in dem anhand einzelner Fahrzeuganalysen ein strukturiertes Vorgehen für Fahrzeugtests entwickelt wurde. Die Untersuchungen hier umfassten unter anderem Angriffe auf Schließsysteme, auf die Diagnoseschnittstelle oder auch auf Infotainmentsysteme. Die Ergebnisse des Projektes sollen in einem Folgeprojekt und in Zusammenarbeit mit anderen Behörden zu einem Leitfaden, der als Planungsgrundlage für praktische Untersuchungen dienen soll, weiterentwickelt werden.

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 BSI seit Dezember 2021 in mehreren Projekten mit dem Technologieunternehmen ZF und der TÜV Informationstechnik GmbH (TÜViT). Ziel dieser Projekte ist die Erprobung und Weiterentwicklung von Anforderungen, Methoden und Werkzeugen für den Bereich des automatisierten Fahrens. Im Projekt AIMobilityAuditPrep wurden zunächst die Rahmenbedingungen und der Stand der Technik analysiert und allgemeine Kriterien und eine erweiterbare Testumgebung entwickelt. Das im Dezember 2022 gestartete Folgeprojekt AIMobilityAudit setzt auf diesen Vorarbeiten auf und hat zum Ziel, die entwickelten Kriterien anhand zweier Anwendungsfälle aus dem automatisierten Fahren umfangreich zu testen und zu konkretisieren. Auf Basis der gewonnenen Erkenntnisse plant das BSI, anschließend 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 erneut verstärkte Aktivitäten. So sieht die KI-Verordnung der EU, die voraussichtlich bis Ende 2023 verabschiedet werden soll, 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, wird seit einiger Zeit vermehrt über KI-Systeme im automatisierten Fahren diskutiert. Perspektivisch könnten diese Diskussionen in einer dedizierten Arbeitsgruppe verstetigt werden.

6 Ausblick

Software in Fahrzeugen

Die neuen technologischen Entwicklungen im Fahrzeugbereich erfordern neben leistungsfähiger Hardware immer umfangreichere und komplexere Software in Fahrzeugen. Einzelfunktionen werden in Zentralsteuergeräten gebündelt, und es kommen vollwertige Betriebssysteme auf diesen zum Einsatz.

Dies ermöglicht es auch, Kundinnen und Kunden nach dem Kauf des Fahrzeugs Zusatzfunktionen per Software-Update über das Infotainment-System anzubieten. Einige Hersteller bieten etwa eine farbige Innenraum-Beleuchtung oder eine Vorklimatisierung als kostenpflichte Upgrades an. Im Zuge dessen sollen entsprechende Bezahlfunktionen in das Fahrzeug integriert werden, etwa über eine biometrische Zwei-Faktor-Authentisierung, bei der der Fingerabdruck geprüft wird (21) (22). Zusätzliche Apps können auch von Drittanbietern stammen.

Entsprechend verzweigt können die Software-Lieferketten ausfallen, was wiederum das Management von Software-Schwachstellen zu einer schwierigen Aufgabe macht.

In vielen Entwicklungsprojekten auch im Transportbereich kommt Open-Source-Code zum Einsatz. Dieser wird häufig von den ursprünglichen Entwicklern nicht fortlaufend gewartet bzw. nicht mehr weiterentwickelt, so dass die Nutzer der Open-Source-Komponenten für die Pflege des Codes verantwortlich sind. In einer Analyse eines Technologieentwicklers von 2023 wurde festgestellt, dass 100 % der untersuchten Codebasen aus dem Transportbereich (einschließlich Luft- und Raumfahrt, Automotive und Logistik) Open-Source-Bestandteile enthielten und dass in 63 % der Fälle „Hochrisiko“-Schwachstellen entdeckt wurden (23). Dies bedeutete einen deutlichen Anstieg der Schwachstellen-Zahlen (über 200 %) gegenüber einer ähnlichen Analyse des Dienstleisters von 2018.

Zu beachten ist jedoch, dass nicht jede Software-Schwachstelle in einem Gesamtsystem wie einem Fahrzeug durch Angreifer ausnutzbar ist. Dies hängt davon ab, in welcher Komponente die betroffene Software implementiert ist und ob ein Angriffsvektor über eine externe Schnittstelle existiert. Nichtsdestoweniger stehen die Hersteller in der Verantwortung, den Gesamtbestand an Software einschließlich der Open-Source-Komponenten in den Produkten fortlaufend auf Schwachstellen zu prüfen und die Auswirkungen derselben auf die Cyber-Sicherheit des Gesamtfahrzeugs festzustellen. Regelmäßige Sicherheitsupdates werden, wie in der klassischen IT, zur Normalität werden.

Offen ist hierbei die Frage, über welchen Zeitraum nach dem Kauf eines Fahrzeugs Patches zur Behebung von Schwachstellen angeboten werden. Die einschlägige Regulierung benennt hier keine konkreten Fristen. Ein großer Automobilhersteller hat angekündigt, den Software-Support über 15 Jahre nach Ende der Produktion zu gewährleisten (24).

Zukünftige Regulierung

Neben den in Kapitel 5 erwähnten bestehenden Regulierungen, Standards und Normen zur Cyber-Sicherheit im Kontext Automotive gibt es noch viele weitere z. T. in der Entwicklung befindliche Vorgaben, die den Automobilsektor betreffen, z. B. den EU AI Act, den EU Data Act, das Cloud-Service-Schema der ENISA und die Ladesäulenverordnung. Insgesamt wird die

Cyber-Sicherheit zunehmend auf europäischer Ebene reguliert. Da die jeweiligen Anwendungsgebiete sich nicht immer klar voneinander abgrenzen lassen, stellen die korrekte Anwendung und technische und praktische Ausgestaltung durch die Industrie und die Kontrolle durch Behörden eine Herausforderung dar.

Ein wichtiges Beispiel für eine solche anstehende Neuregulierung, die wohl auch Auswirkungen auf den Verkehrsbereich haben wird, ist der Cyber Resilience Act der EU.

Beim Cyber Resilience Act (CRA) handelt es sich um eine geplante Harmonisierungsrechtsvorschrift der EU hinsichtlich der Einführung von verpflichtenden Cyber-Sicherheitsanforderungen für Produkte mit digitalen Elementen für das Inverkehrbringen in den Europäischen Binnenmarkt.

Die geplante Regulierung umfasst alle „Produkte mit digitalen Elementen, deren bestimmungsgemäße oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt“ und betrifft somit auch Produkte, die im Kontext des Straßenverkehrs eingesetzt werden (Stand Mai 2023). Es werden allerdings einige Produktkategorien explizit davon ausgenommen, für die bereits andere EU-weite Regelungen gelten. Darunter fallen insbesondere Kraftfahrzeuge und Kraftfahrzeugteile, die unter das Typgenehmigungsrecht nach (EU) 2019/2144 und damit die UN-Regelung 155 fallen. Nicht unter diese Ausnahme fallen wiederum etwa land- und forstwirtschaftliche Fahrzeuge, auf die der CRA nach aktuellem Stand voll anwendbar wird. Ebenso befinden sich Produkte mit digitalen Elementen, die in der Straßeninfrastruktur eingesetzt werden, z. B. Road Side Units für die Fahrzeug-zu-X-Kommunikation im Regelungsbereich des CRA.

In Bezug auf Produktprüfungen werden im CRA u. a. die Kategorien hochkritischer und kritischer Produkte definiert. Hochkritische Produkte erfordern zwingend eine Zertifizierung zur Konformitätsbewertung nach einem Schema unter dem Cyber Security Act (CSA) oder, falls dieses nicht existiert, nach nationalen Zertifizierungsschemata. Die Einstufung, welche Produkte als hochkritisch anzusehen sind, ist bisher nicht erfolgt. Die Einstufung soll nachträglich über einen delegierten Rechtsakt durch die Kommission erfolgen.

Kritische Produkte erfordern i. d. R. eine Konformitätsbewertung nach den Anforderungen des CRA durch eine sog. notifizierte Stelle. Alternativ kann auch eine Zertifizierung nach einem Schema des Cyber Security Acts durchgeführt werden. Für diese gilt dann die Konformitätsvermutung. Beim CRA soll zusätzlich über einen Durchführungsrechtsakt festgelegt werden, welche CSA-Schemata geeignet sind und wie diese im Sinne der Konformitätsvermutung anzuwenden sind.

Jeder Mitgliedsstaat wird verpflichtet, eine nationale Marktüberwachungsbehörde zu benennen. Diese evaluiert auf dem Markt befindliche Produkte und kann im Falle einer Nichtübereinstimmung mit der Regulierung vom Hersteller Korrekturmaßnahmen verlangen oder das weitere Inverkehrbringen untersagen. Hersteller müssen der Behörde auf Verlangen relevante technische Daten, die für Marktüberwachungsaktivitäten erforderlich sind, zur Verfügung stellen.

Die eben genannten Punkte geben den aktuellen Entwurfsstand wieder. Der Cyber Resilience Act wurde in einer Entwurfsfassung im September 2022 von der Europäischen Kommission veröffentlicht. Wichtig zu betonen ist, dass sich der CRA im Zuge der anstehenden weiteren Verhandlungen zwischen Kommission, Parlament und Rat noch deutlich ändern kann. Es wird angestrebt, dass der CRA im ersten Quartal 2024 in Kraft tritt.

Literatur-verzeichnis

1. VDA. [Online] Mai 2023. https://www.vda.de/de/aktuelles/zahlen-und-daten/jahreszahlen/allgemeines.

2. KBA. [Online] Januar 2022. https://www.kba.de/DE/Statistik/Fahrzeuge/Bestand/Jahrebilanz_Bestand/fz_b_jahresbilanz_node.html.

3. Kamkar, Samy. Drive it like you Hacked it. [Online] Dezember 2015. https://www.youtube.com/watch?v=UNgvShN4USU.

4. [Online] Juli 2022. https://rollingpwn.github.io/rolling-pwn/.

5. Levente Csikor, Hoon Wei Lim, Jun Wen Wong, Soundarya Ramesh, Rohini Poolat Parameswarath, Mun Choon Chan. RollBack: A New Time-Agnostic Replay Attack Against the Automotive Remote Keyless Entry Systems. [Online] September 2022. https://arxiv.org/abs/2210.11923.

6. Tindell, Ken. CAN Injection: keyless car theft. [Online] April 2023. https://kentindell.github.io/2023/04/03/can-injection/.

7. Curry, Sam. [Online] Januar 2023. https://samcurry.net/web-hackers-vs-the-auto-industry/.

8. OWASP. [Online] https://owasp.org/www-project-top-ten/.

9. Gordon, Aaron. [Online] Februar 2022. https://www.vice.com/en/article/akvya5/russian-electric-vehicle-chargers-hacked-tell-users-putin-is-a-dickhead.

10. BBC. [Online] April 2022. https://www.bbc.com/news/uk-england-hampshire-61006816.

11. Amariei, Florin. [Online] Januar 2023. https://www.autoevolution.com/news/new-electrify-america-charger-gets-hacked-displays-tesla-s-supercreasing-network-209367.html.

12. ETSI. ETSI TS 103 301, V 1.3.1, „Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services“. 2020.

13. C-Roads Germany. [Online] https://www.c-roads-germany.de/english/c-its-services/tsp/.

14. ISO. ISO/SAE 21434:2021, Road Vehicles — Cybersecurity Engineering. [Online] August 2021. https://www.iso.org/standard/70918.html.

15. —. ISO/PAS 5112:2022, Road Vehicles — Guidelines for auditing cybersecurity engineering. [Online] März 2022. https://www.iso.org/standard/80840.html.

16. KBA. [Online] November 2022. https://www.kba.de/DE/Presse/Pressemitteilungen/Allgemein/2022/pm45_2022_AVP_erste_Genehmigung.html.

17. —. [Online] Oktober 2022. https://www.kba.de/DE/Presse/Pressemitteilungen/Allgemein/2022/pm39_2022_AVP.html.

18. ISO. ISO 23374-1, Intelligent transport systems — Automated valet parking systems (AVPS) — Part 1: System framework, requirements for automated driving and for communications interface. [Online] https://www.iso.org/standard/78420.html.

19. —. ISO/DTS 23374-2, Intelligent transport systems — Automated valet parking systems (AVPS) — Part 2: Security integration for type 3 AVP. [Online] https://www.iso.org/standard/82046.html.

20. European Parliament and the Council. : Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive. 2022.

21. Bellmer, Patrick. [Online] März 2023. https://www.heise.de/news/Volkswagen-kuendigt-App-Store-fuer-Audi-und-weitere-Marken-an-7531000.html.

22. Linden, Michael. [Online] März 2023. https://www.golem.de/news/in-car-payment-mercedes-verkauft-auto-upgrades-per-fingerabdruck-2303-172404.html.

23. Synopsis. Open Source Security and Risk Analysis Report. [Online] April 2023. https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/rep-ossra-2023.pdf.

24. La Rocco, Nicolas. [Online] März 2023. https://www.computerbase.de/2023-03/cariad-vw-will-15-jahre-android-updates-zur-verfuegung-stellen/.

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 2023

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 © ZinetroN, S. 02 und S. 31: AdobeStock © Mopic, Seite 4: AdobeStock © ZinetroN, S. 6/7 oben: AdobeStock © robsonphoto, Seite 7 unten: AdobeStock © Helmut, S. 8: Adobe-Stock © Framestock, Seite 10/11: AdobeStock © Gorodenkoff, S. 12: AdobeStock © kinwun, S. 18: AdobeStock © Gorodenkoff, S. 21: AdobeStock © sdecoret, S. 22: AdobeStock © metamorworks, S. 24: AdobeStock © Yeti Studio

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: 0800 274 1000
E-Mail: bsi@bsi.bund.de
www.bsi.bund.de