September 2020
8. Jahrg.
Seite 81–188

RAW

2

Recht ■ Automobil ■ Wirtschaft
Unternehmen | Technologie | Beratung

dfv Mediengruppe · Frankfurt am Main

Aufsätze

Thomas Kahl und Dr. Philipp Behrendt, Frankfurt a. M./Hamburg*

Datenschutzrechtliche Herausforderungen der Cyber-Abwehr im Connected-Car-Umfeld

I. Einleitung

Das Regelwerk zur Cybersecurity im Fahrzeug der Arbeitsgruppe UNECE WP.29 der Vereinten Nationen (WP.29) sieht vor, dass Automobilhersteller künftig ein *Vehicle Cyber-Security Management-System* (CSMS) implementieren müssen. Die Anforderungen sollen Voraussetzung für die Typengenehmigung und ggf. schon im Jahr 2022[1] verbindlich werden.

Der Schritt scheint konsequent: Cyber-Angriffe auf vernetzte Fahrzeuge können zu erheblicher Gefährdung der Sicherheit der Fahrzeuginsassen und somit der Verkehrssicherheit führen.[2] Die Entwicklungen erhöhen den Druck auf Fahrzeughersteller, zeitnah entsprechende Sicherheitsarchitekturen aufzubauen.

Aus produkthaftungs- und -beobachtungsrechtlicher Sicht gilt dabei oftmals die Devise „mehr Daten, mehr Information, mehr Sicherheit". Dabei ist zur Überwachung der jeweiligen Ökosysteme die Verarbeitung (personenbezogener) Fahrzeugdaten unumgänglich.[3] Wie das Spannungsverhältnis zwischen dem Datenschutz und produkthaftungs- und –beobachtungsrechtlichen Anforderungen aufzulösen ist, beantworten weder die derzeit verfügbaren gesetzlichen Vorgaben, noch die dazu ergangenen aufsichtsbehördlichen Stellungnahmen.

Der folgende Beitrag widmet sich diesem Spannnungsverhältnis und wie es datenschutzkonform aufgelöst werden kann.[4]

II. Cybersecurity im vernetzten Fahrzeug

Cyberangriffe auf das Ökosystem des vernetzten Fahrzeugs können über verschiedenste Angriffswinkel erfolgen. Besonders relevant sind Schnittstellen, über die Hacker sich Zugriff auf die jeweiligen Infrastrukturen verschaffen können (u. a. Bedienschnittstellen im Fahrzeug, die OBD-2-Schnittstelle, Anschlüsse für externe Devices, Remote-Zugänge, drahtlose Kommunikationsschnittstellen wie Bluetooth-, WLAN- oder auch die Mobilfunkverbindung sowie Schnittstellen zum Backend des Fahrzeugherstellers).[5]

Um Cyberangriffe auf das vernetzte Fahrzeug erkennen und managen zu können, sollen sog. *Intrusion-Detection-*(IDS)[6] oder *Security-Information-and-Event-Management-*(SIEM)[7] – Systeme zum Einsatz kommen. Die jeweiligen Systeme und Prozesse werden durch ein *Security Operations Center* (SOC) gemanagt (zusammen nachfolgend vereinfacht als „SIEM" bezeichnet). Kernidee eines SIEM ist die Überwachung der Aktivitäten in – und außerhalb des vernetzten Fahrzeugs, um – regelbasiert, aber zukünftig auch mithilfe von Machine Learning – Aktivitäten und Anomalien zu erkennen, die auf einen Cyberangriff mit potenziell schädlichen Folgen hinweisen.[8]

III. Datenschutzrechtliche Relevanz

Um eine möglichst breite Datenbasis für das SIEM zu erhalten, ist die Verarbeitung von Fahrzeugdaten erforderlich (u. a. Alarm- und Fehlermeldungen, Bordnetznachrichten oder Informationen aus Steuergeräten).[9]

Datenschutzrechtliche Relevanz erlangen die Verarbeitungsvorgänge in der Regel durch die Verknüpfung eines Datensatzes mit der jeweiligen Fahrzeugidentifikationsnummer (FIN),[10] die aus technischen Gründen für die Aus-

---

* Auf Seite III erfahren Sie mehr über die Autoren.

1 Vgl. Art. 4 Abs. 5 i. V. m. Anlage 3, D4 Verordnung (EU) 2019/2144; vgl. auch Press Release der UNECE WP.29 vom 25.6.2020, abrufbar unter https://www.unece.org/info/media/presscurrent-press-h/transport/2020/un-regulations-on-cybersecurity-and-software-updates-to-pave-the-way-for-mass-roll-out-of-connected-vehicles/doc.html (zuletzt abgerufen am 10.7.2020).

2 Vgl. *von Bodungen* in: Handbuch Deutsches und Europäisches Datenschutzrecht, 2019, § 16, Rn. 50 m. w. N..

3 Vgl. *Simo/Waidner/Geminn,* in: Roßnagel/Hornung (Hrsg.), Grundrechtsschutz im Smartcar, Wiesbaden, 2019, 314, 331.

4 Vgl. zu den technischen Hintergründen *Simo/Waidner/Geminn,* 314, 331 ff..

5 Vgl. Security Insider, Automotive Security Operation Center, 9.1. 2019, abrufbar unter https://www.security-insider.de/amp/digitale-wachposten-fuer-das-connected-car-a-785094/ (zuletzt abgerufen am 10.7.2020); *Simo/Waidner/Geminn,* in: Roßnagel/Hornung (Fn. 3), S. 314.

6 Vgl. *Simo/Waidner/Geminn,* in: Roßnagel/Hornung (Fn. 3), 314.

7 Vgl. Security Insider, Was ist ein SIEM, 6.11.2018, abrufbar unter https://www.security-insider.de/was-ist-ein-siem-a-772821/ (zuletzt abgerufen am 13.7.2020).

8 Vgl. *Simo/Waidner/Geminn,* in: Roßnagel/Hornung (Fn. 3), 314, 329.

9 Vgl. Security Insider, Automotive Security Operation Center, 9.1.2019 (Fn. 5).

10 Vgl. zum Personenbezug der FIN die Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA), „Daten-

wertung der Datensätze im SOC erforderlich sein und gleichzeitig eine Rückverfolgbarkeit auf das betroffene Fahrzeug im Fall einer besonderen Gefahrensituation ermöglichen kann.[11]

IV. Der rechtliche Rahmen für Cybersecurity im vernetzten Fahrzeug

1. Spezielle Anforderungen im Automotive-Sektor

Die Taskforce TF-CS/OTA der UNECE-WP.29-Arbeitsgruppe zum autonomen Fahren (GRVA) hat bereits in den Jahren 2019/2020 verschiedene UNECE-Regulierungsentwürfe zur Vehicle Cybersecurity vorgelegt.[12] Nach den Vorgaben müssen Automobilhersteller zukünftig ein zertifiziertes CSMS implementieren und über den kompletten Lebenszyklus des Fahrzeugs aufrecht erhalten.[13] Die Vorgaben stellen Hersteller vor besondere Herausforderungen, insbesondere weil Cyber-Risiken im Zeitpunkt der Konzeption des Fahrzeugs und seiner Sicherheitsmechanismen oft nur bedingt vorhersehbar sein werden.[14] Die Umsetzung und der Nachweis der Vorgaben durch Zertifizierung wird zur Voraussetzung der Fahrzeugtypzulassung und für Automobilhersteller (voraussichtlich) ab Juli 2022 verbindlich.[15] Die Anforderungen werden durch den parallel im Entwurf veröffentlichten SAE/ISO-Industriestandard 21434 zu Cybersecurity konkretisiert.[16]

2. Branchenunabhängige Regelungen zur IT-Sicherheit

Daneben existieren verschiedene branchenunabhängige Vorgaben an die IT-Sicherheit, die ebenso für die Cybersecurity im Fahrzeug von Relevanz sind.

Die im Juni 2019 in Kraft getretene Cybersecurity-Verordnung (EU) 2019/881 regelt Anforderungen an die Cybersicherheit von Produkten und Dienstleistungen, u. a. die Etablierung einer Cyber-Zertifizierung für IT-Produkte.[17]

Das BSI-Gesetz (BSIG) regelt bestimmte Anforderungen an Betreiber sog. kritischer Infrastrukturen (KRITIS), die derzeit für Automobilhersteller (wohl) keine unmittelbare Wirkung entfalten. Dies mag sich mit Inkrafttreten eines IT-Sicherheitsgesetzes 2.0[18] ändern, soweit darunter auch Unternehmen von erheblicher volkswirtschaftlicher Bedeutung reguliert werden sollen (vgl. § 2 Abs. 14 IT-SIG 2.0). Entsprechende Vorgaben sind jedoch heute (noch) nicht in Kraft.

3. Datenschutzrechtliche Vorgaben

Vorgaben zur Datensicherheit finden sich zudem in den allgemeinen Regelungen der DS-GVO[19], u. a. in Art. 32, 25. Konkretisiert werden die jeweiligen Vorgaben durch einzelne Stellungnahmen von Datenschutzaufsichtsbehörden, für den Automotive-Bereich, u. a. die Stellungnahme der französischen Datenschutzaufsicht CNIL[20] und der Draft (not adopted) des European Data Protection Board (EDPB)[21], die sich mit dem Datenschutz im Umfeld vernetzter Fahrzeuge befassen. Die Guidelines beinhalten ihrerseits einzelne, aber noch wenig konkrete Vorgaben für die Ausgestaltung entsprechender Cybersecurity-Systeme.

V. Cybersecurity aus produkthaftungs- und -beobachtungsrechtlicher Sicht

1. Allgemeines zu den Verkehrssicherungspflichten des Herstellers

Sowohl die Produktbeobachtungspflicht als auch die Pflicht zur effektiven Gefahrsteuerung sind Aspekte der produzentenhaftungsrechtlichen Verkehrssicherungspflichten des Fahrzeugherstellers. Unter diesen Oberbegriff wird eine Vielzahl verschiedener, nicht gesetzlich normierter, aber von der Rechtsprechung entwickelter Pflichten sortiert, die sich sämtlich auf den Zeitraum nach dem In-Verkehr-Bringen eines Produktes beziehen.[22] Im Rahmen seiner Verkehrssicherungspflicht ist der Hersteller auch nach diesem Zeitpunkt verpflichtet, „alles zu tun, was ihm nach den Umständen zumutbar ist, um Gefahren abzuwenden, die sein Produkt erzeugen kann."[23]

Der Pflichtenkreis des Herstellers geht also dahin, dass er sämtliche nach dem aktuellen Stand der Technik verfügbaren Maßnahmen zur Gewährleistung der Sicherheit seines Produkts – soweit im Verhältnis zum gesetzten Risiko zumutbar – einsetzen muss. Neben den eingangs erwähnten Produktbeobachtungspflichten sowie der Pflicht zur effektiven Gefahrsteuerung fallen unter diesen Pflichtenkreis zum Beispiel die vorgelagerten Pflichten zur fehlerfreien Konstruktion und Fabrikation sowie zur angemessenen Instruktion. Im Bereich von Connected Cars und der mit den technischen Entwicklungen einhergehenden neuen Möglichkeiten zur Datenanalyse und zum Remote-Zugriff stehen die eingangs erwähnte Produktbeobachtungspflicht

schutzrechtliche Aspekte bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge" vom 26.1.2016, 2, abrufbar unter https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2016/ErklaerungDSK_VDA_VernetzteKfz.html;jsessionid=7EE3B6F19FDD76493C56102E294AAD49.2_cid354?nn=5217320 (zuletzt abgerufen am 10.7.2020).

11 Eine vollständig anonymisierte Verarbeitung dürfte in den meisten Fällen ausscheiden. So wohl i. E. auch *Simo/Waidner/Geminn,* in: Roßnagel/Hornung (Fn. 3), 330.

12 Vgl. u. a. UNECE-Regulierungsentwurf zur Vehicle Cybersecurity, Version vom 23.6.2020, abrufbar unter http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf (zuletzt abgerufen am 10.7.2020).

13 Vgl. UNECE-Regulierungsentwurf zur Vehicle Cybersecurity, Version vom 23.6.2020 (Fn. 12), Ziffer 6.10.

14 Vgl. *Langer,* RAW 2017, 103, 104.

15 Vgl. Richtlinie 2007/46/EG sowie Art. 4 Abs. 5 i. V. m. Anlage 3, D4 der Verordnung (EU) 2019/2144. Gem. UNECE-Regulierungsentwurf zur Vehicle Cybersecurity, Version vom 23.6.2020 (Fn. 12), Ziffer 7.3.1, ist für bestimmte Fallgestaltungen eine Übergangsfrist bis zum 1.7.2024 vorgesehen.

16 ISO/SAE DIS 21434: Road vehicles – Cybersecurity engineering, verfügbar auf den Webseiten der ISO unter https://www.iso.org/standard/70918.html (zuletzt abgerufen am 14.7.2020).

17 Vgl. Art. 49, 56 Verordnung (EU) 2019/881.

18 Vgl. Referentenentwurf des BMI vom 27.3.2019, abrufbar unter http://intrapol.org/wp-content/uploads/2019/04/IT-Sicherheitsgesetz-2.0-_-IT-SiG-2.0.pdf (zuletzt abgerufen am 9.7.2020).

19 Artikel ohne Gesetzesangaben sind solche aus der DS-GVO.

20 Vgl. CNIL, Connected Vehicle Compliance Package vom 13.2.2018, abrufbar unter https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf (zuletzt abgerufen am 10.7.2020).

21 Vgl. Draft EDPB Guidelines 1/2020 zu Connected Vehicles vom 28.1.2020, abrufbar unter https://edps.europa.eu/sites/edp/files/publication/2019-12-29_techdispatch-3_connected-cars_en_2.pdf (zuletzt abgerufen am 10.7.2020).

22 Hierin liegt auch der Unterschied zur (verschuldensunabhängigen) Produkthaftung nach §§ 1 ff. ProdHaftG, vgl. *Grünvogel/Dörrenbächer,* ZVertriebsR 2019, 87, 88.

23 BGH, Urteil v. 16.12.2008 – VI ZR 170/07, NJW 2009, 1080; BGH, Urt. v. 16.9.2009 – VI ZR 107/08 – Airbag.

und die Pflicht zur effektiven Gefahrsteuerung im Fokus. Schließlich nehmen die Erwartungen an die Sicherheit mit der steigenden Vernetzung und den durch diese gesteigerten Sicherheitsrisiken zu.[24] Kommt der Hersteller seiner Produktbeobachtungspflicht nicht ausreichend nach und kann dementsprechend nicht rechtzeitig reagieren, um die von dem Produkt für den Kunden ausgehende Gefahr abzuwenden bzw. effektiv zu steuern, so haftet er für den infolge dieser Verletzung der Verpflichtung zur Reaktion entstandenen Schaden nach § 823 Abs. 1 BGB.

2. Produktbeobachtungspflicht

Die Produktbeobachtungspflicht erweitert die Verantwortung des Herstellers für sein Produkt in zeitlicher Hinsicht.[25] Der Hersteller ist verpflichtet, sein Produkt aus Produktsicherheitsperspektive auch nach Inverkehrbringen zu beobachten und – bei Feststellung etwaiger Gefahren – Gefahrsteuerungsmaßnahmen zu ergreifen (hierzu sogleich). Hierin liegt eine Pflicht des Herstellers zur Selbstinformation, da sie die Grundlage für die anschließenden Reaktionspflichten bildet.[26] Er darf sich nicht darauf verlassen, „mehr oder weniger zufällig" von etwaigen Gefahren seines Produkts zu erfahren, sondern muss vielmehr bereits die notwendigen organisatorischen Voraussetzungen schaffen, dass technische und wissenschaftliche Entwicklungen, praktische Verwendungsfolgen sowie Schadensmeldungen ihm nicht entgehen.[27] Die Produktbeobachtungspflicht korrespondiert im Falle einer festgestellten Gefahr mit der Pflicht, die Gefahr effektiv abzuwenden. Intensität der und Umgang mit den zu ergreifenden Maßnahmen hängen einerseits vom Rang des gefährdeten Rechtsguts sowie dem Ausmaß des drohenden Schadens und andererseits von der Möglichkeit und Zumutbarkeit der Maßnahmen für den Hersteller ab.[28]

3. Spezielle Fragestellungen im Zusammenhang mit „Connected Cars"

a) Produktsicherheitsrechtliche Pflicht zur Auswertung mittels Analysetools unter Zuhilfenahme von Fahrzeugdaten

Bei Connected Cars hat der Hersteller die technische Möglichkeit, auch nach Übergabe an den Kunden den Zustand eines Gerätes sowie etwaige Störungen/Fehler der jeweiligen Produkte zu überwachen. Hypothetisch ermöglichen diese neuen Formen des Remote Data Access, Produktbeobachtungspflichten um ein Vielfaches effektiver zu erfüllen.[29] Ob sich aus dieser *theoretischen* Möglichkeit der Informationsgewinnung jedoch im Gegenschluss auch eine dahingehende *Pflicht* des Herstellers herleiten lässt, wird derzeit kontrovers diskutiert. Für eine Pflicht zur Sammlung und Auswertung sicherheitsrelevanter Daten wird angeführt, dass Fehler auf diese Weise früher erkannt werden könnten als mit „herkömmlichen" Methoden der Informationsgewinnung.[30] Ergänzend wird angeführt, dass gerade eine potenzielle Gefahr für Leib und Leben eine intensive Kontrolle des auf dem Markt befindlichen Fahrzeugs als „unerlässlich" erscheinen lasse.[31] Gegen diese Auffassung ließe sich anführen, dass hierdurch die Grenzen zwischen Produzentenhaftung und Sachmängelrecht verwischt würden, woraus sich die Unzumutbarkeit für die Hersteller ergebe.[32] Jedenfalls werden bei der Umsetzung einer solchen „Pflicht zur Einsichtnahme" dennoch die datenschutzrechtlichen Grenzen eingehalten werden müssen, was sicherlich die größte rechtliche Hürde in diesem Zusammenhang darstellt.[33] Im Ergebnis wird man gerade bei Connected Cars aufgrund der Sicherheitsrelevanz und der potenziellen Gefahr für Leib und Leben nicht ausschließen können, dass ein Hersteller deliktisch haftet, der eine mögliche und zumutbare Nutzung unterlässt. In diese Richtung deuten auch die Vorgaben des UNECE-Regulierungsentwurfs zu Vehicle Cybersecurity, der ein entsprechendes Monitoring des Fahrzeugs bzw. seiner Funktionen ausdrücklich zur Voraussetzung der Zulassung macht.[34]

b) Exkurs: Pflichten zur Bereitstellung von Updates oder Produktstilllegung per Remote-Zugriff

Eine weitere derzeit noch kontrovers diskutierte Frage ist, ob ein Hersteller bei Bekanntwerden insb. von Sicherheitslücken bestimmter vernetzter Produkte im Rahmen seiner Verkehrssicherungspflichten[35] verpflichtet ist, entsprechende Software-Updates zur Schließung der Sicherheitslücken (kostenlos) zur Verfügung zu stellen[36] oder sogar zur Stilllegung eines Fahrzeugs per Remote-Steuerung verpflichtet sein kann.

Der Themenkreis soll an dieser Stelle nicht weiter vertieft werden und bedarf – wie auch die damit verbundenen datenschutzrechtlichen Implikationen – einer umfassenderen Betrachtung an anderer Stelle. Will man sich dem Thema nähern, liefert eine Parallelwertung zum Produktrückruf jedoch erste Anhaltspunkte.[37]

---

24 *Raith,* Das vernetzte Automobil (Diss.), 2019, S. 43; wie *Fleck/Thomas,* NJOZ 2015, 1393, 1397 ausführen, werden sie noch höher sein, wenn es zum hoch- bzw. vollautomatisierten Fahren kommt.

25 *Grünvogel/Dörrenbächer,* ZVertriebsR 2019, 87, 88; *Wagner,* in: MüKo BGB, 7. Auflage 2017, § 823, Rn. 837.

26 Vgl. *Wagner,* in: MüKo BGB, 7. Aufl. 2017, Rn. 840.

27 *Raith* (Fn. 24), S. 47 mit Verweis auf BGH, Urt. v. 17.3.1981 – VI ZR 286/78, NJW 1981, 1606 (1608). Der Hersteller haftet allerdings nicht für sog. „Entwicklungsrisiken", also für solche Risiken, die sich aus dem Umstand ergeben können, dass das Produkt *nicht mehr* dem Stand der Technik und Wissenschaft entspricht. Das Produkt muss vielmehr grundsätzlich nur zum Zeitpunkt des Inverkehrbringens diesem Stand entsprechen, siehe *Raith* (Fn. 24), S. 47; *Wagner,* in: MüKo BGB, 7. Aufl. 2017, § 823 BGB, Rn. 817; *Förster,* in: BeckOK-BGB, 52. Ed., § 823, Rn. 731, 733 m. w. N..

28 *Wagner,* in: MüKo, § 823 BGB, Rn. 838; *Grünvogel/Dörrenbächer,* ZVertriebsR 2019, 87, 88.

29 *Grünvogel/Dörrenbächer,* ZVertriebsR 2019, 87, 89.

30 *Grünvogel/Dörrenbächer,* ZVertriebsR 2019, 87, 89; *Piltz/Reusch,* BB 2017, 841, 842.

31 *Droste,* CCZ, 2015, 105, 107.

32 *Grünvogel/Dörrenbächer,* ZVertriebsR 2019, 87, 89.

33 *Grünvogel/Dörrenbächer,* ZVertriebsR 2019, 87, 89 mit Verweis auf *Droste,* CCZ, 2015, 105, 110; eingehend *Piltz/Reusch,* BB 2017, 841, 842.

34 Vgl. UNECE-Regulierungsentwurf zur Vehicle Cybersecurity, Version vom 23.6.2020, Ziffer 7.2.2.2. (g) (Fn. 12): „The processes used to monitor for, detect and respond to cyber-attacks, cyber threats and vulnerabilities on vehicle types and the processes used to assess whether the cyber security measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified."

35 Im Folgenden wird nicht auf etwaige vertragsrechtliche Verpflichtungen der Hersteller zur Bereitstellung eingegangen.

36 Das ProdHaftG scheidet – wie eingangs erwähnt – als Grundlage einer Update-Pflicht aus, weil es „seiner Konzeption nach keine Nachmarktphase kennt, sondern alleine auf die Sicherheit zum Zeitpunkt der Inverkehrgabe abstellt", siehe *Reusch,* BB 2019, 904, 908.

37 *Grünvogel/Dörrenbächer,* ZVertriebsR 2019, 87, 89; *Reusch,* BB 2019, 904, 908; *Schrader/Engstler,* MMR 2018, 356, 360; zur deliktischen Pflicht zum Produktrückruf siehe statt vieler nur *Lüftenegger,* NJW 2018, 2087.

Unter welchen Voraussetzungen eine (deliktsrechtliche) Pflicht des Herstellers zum Produktrückruf per Remote-Zugriff besteht, ist höchst umstritten.[38] In Anwendung der Grundsätze der Rechtsprechung des BGH[39] dürfte die Produzentenhaftung grundsätzlich nur in einer Pflicht zur Warnung bestehen, einen bestimmten Dienst nicht (mehr) zu nutzen, wenn hierdurch die Gefahr effektiv beseitigt werden kann.[40] Für die Bereitstellung von Updates wird das jedoch u. a. durch Verweis auf den geringeren Aufwand vielfach anders gesehen.[41] Wenn die Zurverfügungstellung des Updates kaum Aufwand für den Hersteller bedeutet, wird sie auch zumutbar sein, sodass eine entsprechende Pflicht ggf. schon aus produzentenhaftungsrechtlichen Erwägungen heraus geboten sein kann.

Dies deckt sich auch mit den Ansätzen der UNECE-WP.29-Regularien, die die Implementierung eines Cyber-Management-Systems fordern, das über den gesamten Lebenszyklus des Fahrzeugs die Behebung von Schwachstellen der IT-Sicherheit ermöglichen soll ohne dabei allerdings konkreter zu werden.[42]

Zur Produktdeaktivierung per Remote-Access dürfte Folgendes zu beachten sein:

Nach der Rechtsprechung des BGH besteht für den Hersteller auf Basis seiner Verkehrssicherungspflichten nur im Ausnahmefall eine Verpflichtung, gefährliche Produkte aus dem Verkehr zu ziehen.[43] Im Kontext von Connected Cars und allgemein Smart Devices ergibt sich die Besonderheit, dass ein Produktrückruf nicht mehr zwingend mit größtem Aufwand verbunden ist, sondern – je nach technischer Ausgestaltung – „per Maus-Klick" möglich sein kann und insbesondere keine Mitwirkung des Eigentümers/Verbrauchers erfordert.

Einem solchen Vorgehen sind allerdings (eigentumsrechtliche) Grenzen gesetzt: Jedenfalls die Stilllegung intelligenter Hausgeräte, die zur vollständigen oder nahezu vollständigen Aufhebung der Verwendungsfähigkeit des Smart Devices führt, stellt einen Eingriff in das gem. § 823 Abs. 1 BGB geschützte Eigentumsrecht dar[44], die im Verhältnis zum Eigentümer der Rechtfertigung bedarf. Allenfalls eine Rechtfertigung gem. § 228 S. 1 BGB (Defensivnotstand) wäre denkbar. In einem solchen Fall muss dann aber über die Erforderlichkeit hinaus auch die Verhältnismäßigkeit der jeweiligen Deaktivierung gewahrt sein. Kann daher die Gefahr durch die zuvor beschriebenen Updates, andere Maßnahmen oder mindestens die Deaktivierung einzelner Produktfunktionen behoben werden, wäre eine vollständige Deaktivierung nicht mehr verhältnismäßig.

So bleibt festzuhalten, dass der Hersteller eines Connected Vehicle die sich aus der Vernetzung ergebenden Möglichkeiten zur Produktbeobachtung grundsätzlich wird nutzen müssen. Grenzen werden ihm dabei u. a. durch den Datenschutz gesetzt. Gewinnt der Hersteller Erkenntnisse über Gefahren, wird er auch zur Reaktion verpflichtet sein. Die Bereitstellung von Updates wird sicherlich in gewissem Umfang verpflichtend sein, die Stilllegung des Fahrzeuges per Remote Access eher in Ausnahmefällen.

VI. Datenschutzrechtliche Rechtfertigungsansätze

Die Verarbeitung personenbezogener Fahrzeugdaten für Zwecke des SIEM bedarf einer datenschutzrechtlichen Erlaubnis (vgl. Art. 5 Abs. 1 lit. a).

1. Vorüberlegungen

a) Generelle „Showstopper"

Die im Februar 2020 veröffentlichte Konsultationsfassung der Connected Vehicles Guidelines des EDPB[45] geben Anlass zu der Frage, ob für die Datenverarbeitung für Zwecke eines SIEM datenschutzrechtliche „Showstopper" existieren.

Eine erste Hürde könnte sich aus der vom EDPB favorisierten Anwendung von Art. 5 Abs. 3 der ePrivacy-Richtlinie[46] auf Fahrzeugdaten ergeben. Danach soll die Verarbeitung von Fahrzeugdaten in vielen Fällen auf eine Einwilligung gestützt werden.[47]

Das scheint aus mehreren Gründen fragwürdig. Unklar ist schon, ob das EDPB bei seinen Äußerungen Datenverarbeitungen für Zwecke der Cybersecurity vor Augen hatte.[48] Empfiehlt das EDPB an anderer Stelle selbst ein Datenmonitoring zur Identifizierung von Cyber-Angriffen,[49] würde diese Empfehlung bei gleichzeitigem Einwilligungsvorbehalt weitestgehend leerlaufen.

Weitere Zweifel ergeben sich im Hinblick auf das Verhältnis zwischen der geltenden ePrivacy-Richtlinie und der DS-GVO bzw. dem in Deutschland geltenden Telemediengesetz (TMG).[50]

Mit Blick auf die geplante ePrivacy-Verordnung wird vielmehr klar, dass man erkannt haben dürfte, dass eine Öffnung für flexiblere Lösungen erforderlich ist. So sieht ein aktuellerer Entwurf für eine ePrivacy-VO die Speicherung und Abfrage von Informationen auf „Endgeräten" auch auf Grundlage einer Interessenabwägung vor und erwähnt als berechtigtes Interesse sogar Sicherheitsaspekte.[51]

38 Siehe statt vieler nur *Lüftenegger,* NJW 2018, 2087.
39 BGH, Urteil v. 16.12.2008 – VI ZR 170/07, NJW 2009, 1080.
40 *Schrader,* NZV 2018, 489, 493.
41 *Raue,* NJW 2017, 1841, 1844; *Droste,* CCZ, 2015, 105, 108, 110; *Grünvogel/Dörrenbächer,* ZVertriebsR 2019, 87, 89 m. w. N.
42 Vgl. UNECE-Regulierungsentwurf zu Vehicle Cybersecurity, Version vom 23.6.2020 (Fn. 12), S. 8 ff., insbesondere Ziffer 7.2.2.3; so wohl auch CNIL, Connected Vehicle Compliance Package vom 13.2.2018 (Fn. 20), in dem u. a. folgende Maßnahmen vorgesehen werden: „implementing technical measures that enable to rapidly patch security vulnerabilities", die jedoch i. E. wohl aus Art. 32, 25 hergeleitet werden.
43 *Grünvogel/Dörrenbächer,* ZVertriebsR 2019, 87, 90.
44 *Grünvogel/Dörrenbächer,* ZVertriebsR 2019, 87, 90. Kommt es hingegen nur zu einer partiellen Stilllegung, d. h. werden nur bestimmte, untergeordnete Gerätefunktionen abgeschaltet, soll hierin nach Auffassung der Autoren kein Eingriff in das gem. § 823 Abs. 1 BGB geschützte Eigentumsrecht liegen.
45 EDPB, Guidelines 1/2020 zu Connected Vehicles (Fn. 21).
46 Richtlinie 2002/58/EG vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).
47 Vgl. EDPB, Guidelines 1/2020 zu Connected Vehicles (Fn. 21), Rn. 9 ff..
48 Unklar ist, inwieweit das EDPB die Verarbeitung für Cybersecurity-Zwecke unter die Ausnahmen in Art. 5 (3) S. 2 der Richtlinie fassen würde (Erforderlichkeit für die Erbringung eines Dienstes der Informationsgesellschaft), was an dieser Stelle nicht weiter untersucht werden soll.
49 Vgl. EDPB, Guidelines 1/2020 zu Connected Vehicles (Fn. 21), Rn. 91.
50 So i. E. wohl auch die Stellungnahme des ACEA im Rahmen der Konsultation des EDBP, dort S. 8, abrufbar unter https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-12020-processing-personal-data-context_de (zuletzt abgerufen am 10.7.2020), worauf hier aber nicht weiter eingegangen werden soll.
51 Vgl. Entwurf der kroatischen Ratspräsidentschaft vom 21.2.2020, S. 15, abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5979_2020_INIT (zuletzt abgerufen am 10.7.2020) sowie den dazugehörigen Progress Report vom 29.5.2020 mit Verweis auf zwischenzeitliche weitere, teils auch kritische Stellungnahmen, abrufbar unter https://www.consilium.europa.eu/media/44301/st_8204_2020_init_en.pdf (zuletzt abgerufen am 10.7.2020).

Fraglich scheint zudem die Bedeutung von Art. 10 DS-GVO für SIEM-Prozesse, wenn und weil damit Verhalten aufgedeckt bzw. erfasst werden könnte, das strafrechtlich relevant sein kann.[52]

Der Anwendungsbereich von Art. 10 wird zu Recht ganz überwiegend restriktiv verstanden und erstreckt sich (wohl) nicht auf den privaten Bereich.[53] Die Stellungnahme des EDPB erstaunt insoweit. Fordert das EDPB an anderer Stelle selbst das Monitoring von Fahrzeugzugriffen, um (rechtswidrige) Cyberattacken nachvollziehen zu können, dürfte sich eine derart umfassende Anwendung des Art. 10 nicht mit dieser Empfehlung vereinbaren lassen. Die Erläuterungen sind wohl in diesem Lichte zu lesen.

Perspektivisch sollten somit weder Art. 5 Abs. 3 der ePrivacy-Richtlinie noch Art. 10 eine generelle Hürde für die Implementierung entsprechender Prozesse darstellen. Alles andere schiene fragwürdig. Automobilhersteller werden die Entwicklung jedoch weiterhin aufmerksam beobachten (müssen).

2. (Wohl) Weniger relevante Erlaubnistatbestände

Auch wenn es danach einer Einwilligung (vgl. Art. 6 Abs. 1 lit. a) für ein SIEM nicht generell bedürfen wird, könnte die Datenverarbeitung theoretisch trotzdem auf eine solche gestützt werden. Das dürfte für SIEM-Prozesse aber aus mehreren Gründen wohl nie ernsthaft in Betracht kommen. Neben der fehlenden Praxistauglichkeit (Stichwort „Widerruflichkeit“) dürfte sie insbesondere bei solchen Nutzern, mit denen der Hersteller kein direktes (Vertrags-)Verhältnis unterhält, schwer einzuholen sein. Zuletzt dürfte der Einsatz einer Einwilligung mit den bestehenden rechtlichen Anforderungen zur Produktüberwachung kollidieren (vgl. hierzu zuvor unter V.).

Gleiches dürfte für eine Lösung über Art. 6 Abs. 1 lit. b (Vertragserfüllung) gelten.

Für den Großteil der Fälle wird bei Licht besehen auch Art. 6 Abs. 1 lit. d (lebenswichtige Interessen) nicht in Frage kommen. Der Unionsgesetzgeber hatte mit Art. 6 Abs. 1 lit. d offenbar andere Fälle vor Augen. Die Norm dürfte nur dort einschlägig sein, wo bereits eine konkrete Gefahrensituation eingetreten ist[54]. Die (proaktive) Überwachung der Cybersicherheit im Fahrzeug dürfte dem eher nicht unterfallen.

3. Gesetzliche Pflicht (Art. 6 Abs. 1 lit. c)

Wie gesehen, sind Fahrzeughersteller ggf. verpflichtet, Fahrzeugdaten in gewissem Umfang auszuwerten, um die Produktsicherheit auch nach dem Inverkehrbringen gewährleisten zu können (vgl. zuvor V.).

Um eine Verarbeitung auf Basis von Art. 6 Abs. 1 lit. c rechtfertigen zu können, bedarf es jedoch einer ausdrücklichen und konkreten Pflicht zur Datenverarbeitung, die in der einschlägigen Norm selbst beschrieben sein muss.[55]

Ob die aus § 823 BGB hergeleiteten Produktbeobachtungspflichten als ungeschriebenes Recht diesen Anforderungen genügen, scheint danach zumindest fraglich.[56] Gleiches gilt für Art. 32, 25, die selbst keine Vorgaben zu konkreten Datenverarbeitungsmaßnahmen enthalten.[57]

Anders könnte das im Fall der UNECE (WP.29)-Regelungen zu bewerten sein, die bereits in einer gewissen Detailtiefe Datenverarbeitungsvorgänge beschreiben.[58] Für Datenverarbeitungshandlungen, die in den Normen beschrieben werden, scheint eine Einordnung als „rechtliche Verpflichtung“ i. S. d. Art. 6 Abs. 1 lit. c somit auf den ersten Blick zumindest möglich. Das Verhältnis der UNECE-Regelungen zur DS-GVO scheint aber ungeklärt.[59]

Dabei darf nicht außer Acht gelassen werden, dass die Normen derzeit (noch) keine Wirkung entfalten und erst ab verbindlicher Geltung in Europa überhaupt zu einer tauglichen Rechtsgrundlage i. V. m. Art. 6 Abs. 1 lit. c werden könnten.

Zumindest für Verarbeitungshandlungen im SIEM, die sich nicht unmittelbar aus den UNECE-Regelungen ableiten lassen oder (nur) in Erfüllung der Anforderungen ungeschriebener (Rechts-) Pflichten erfolgen, dürfte der Weg über Art. 6 Abs. 1 lit. c erschwert sein. Im Übrigen scheint die Rechtslage ungeklärt. Klarstellungen im weiteren Normsetzungsverfahren wären wünschenswert.

4. Interessenabwägung (Art. 6 Abs. 1 lit. f)

Angesichts dieser Umstände kommt Art. 6 Abs. 1 lit. f für SIEM eine wesentliche Bedeutung zu.

Die praktischen Nachteile im Vergleich zu einer Lösung über Art. 6 Abs. 1 lit. c dürften im Ergebnis überschaubar bleiben: Das im Rahmen der Rechtfertigung über Art. 6 Abs. 1 lit. f bestehende Widerspruchsrisiko dürfte bei datenschutzkonformer Ausgestaltung des SIEM nur eine untergeordnete Rolle spielen. Zudem wird die konkrete Ausgestaltung eines SIEM-Systems unter Art. 6 Abs. 1 lit. c wie Art. 6 Abs. 1 lit. f. ähnlichen Kriterien zu folgen haben. Die nachfolgenden Erwägungen wären somit auch für eine Lösung über Art. 6 Abs. 1 lit. c relevant.

Die Prüfung im Rahmen der Interessenabwägung lässt sich nach den zu Art. 6 Abs. 1 lit. f entwickelten Grundsätzen grob als eine „3-Stufen-Prüfung“ skizzieren. Auf der Stufe der eigentlichen Abwägung sind sodann verschiedene Aspekte zu berücksichtigen, u. a. Art und Gewicht des Interesses an dem mit der Datenverarbeitung verfolgten Zweck

52 Vgl. EDPB Guidelines zu Connected Vehicles (Fn. 21), Rn. 64, 65.

53 Vgl. *Nolde,* in: Taeger/Gabel, DSGVO – BDSG, 3. Aufl. 2019, Art. 10 DSGVO Rn. 9 ff. m. w. N..

54 Statt vieler nur *Schantz,* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 6 Rn. 62.

55 Vgl. *Buchner/Petri,* in: Kühling/Buchner, DS-GVO BDSG, 2. Aufl. 2018, Art. 6 Rn. 76; ferner *Herberlein,* in: Ehmann/Selmayr, Art. 6 Rn. 15: „hinreichend klar, präzise und vorhersehbar“.

56 Anders i. E. wohl der LfDI Baden-Württemberg, 34. Tätigkeitsbericht, 95: „Die datenschutzrechtliche Grundlage für die Datenverarbeitung der erforderlichen Fahrzeugdaten für die Produktüberwachung/ Produktbeobachtung und für eventuelle Rückrufaktionen ist Artikel 6 Absatz 1 Buchstabe c DS-GVO. Es liegt hier die Erfüllung einer rechtlichen Verpflichtung des Automobilherstellers aus dem Produkthaftungsgesetz vor“; vgl. hierzu auch Piltz/Reusch, BB 2017, 841, 846, die eine entsprechende Verarbeitung i. E. wohl als Fall des Art. 6 Abs. 1 lit. b ansehen.

57 Anders könnte dieser Aspekt bewertet werden, würde man Art. 32 i. V. m. einem entsprechenden Standard (z. B. einer ISO-Norm), der ausreichend detaillierte Vorgaben macht, genügen lassen, was denkbar erscheint, an dieser Stelle aber nicht weiter vertieft werden soll.

58 Vgl. UNECE-Regulierungsentwurf zu Vehicle Cybersecurity, Version vom 23.6.2020 (Fn. 12), dort u. a. Ziff. 7.2.2.4.

59 Vgl. UNECE-Regulierungsentwurf zur Vehicle Cybersecurity, Version vom 23.6.2020 (Fn. 12), Ziffer 1.3 und 7.2.2.4 lit. b). So scheinen die Regularien ihren Anwendungsbereich selbst unter den Vorbehalt der Vereinbarkeit der jeweiligen Maßnahmen mit dem anwendbaren Datenschutzrecht zu stellen. Dieser Aspekt soll hier jedoch nicht weiter vertieft werden.

(z. B. Überschneidung mit Allgemeininteressen), Folgen eines Ausbleibens der Verarbeitung für den Verantwortlichen bzw. Dritten, objektive Erwartungen des Betroffenen, die Sensibilität der verarbeiteten Daten oder die Art und Weise der Verarbeitung.[60]

Dabei werden sich für SIEM-Prozesse Beschränkungen u. a. aus den allgemeinen datenschutzrechtlichen Prinzipien der Art. 5, 25 und 32 ergeben.

Die Interessenabwägung dürfte regelmäßig dort positiv ausfallen, wo hochrangige Rechtsgüter (Leib und Leben) geschützt werden und eine ausreichende Wahrscheinlichkeit für den Schadenseintritt besteht.

Dabei sind rechtliche Verpflichtungen des Herstellers, die nicht bereits über Art. 6 Abs. 1 lit. c berücksichtigt werden können, maßgeblich in die Abwägung einzustellen. Bestehen solche, werden diese oftmals Indizwirkung für eine positive Interessenabwägung haben, wenn sich die Verarbeitung im Übrigen innerhalb der datenschutzrechtlichen „Leitplanken" bewegt.

VII. Leitplanken und Gestaltungsmöglichkeiten

1. Datenminimierung und Erforderlichkeit „by Design"

Beim Design der jeweiligen Prozesse sind zuvorderst die Grundsätze der Erforderlichkeit und Datenminimierung (vgl. Art. 5 Abs. 1 lit. c) zu beachten. Zu trennen ist zwischen den Prozessen im Fahrzeug, der Erhebung aus dem Fahrzeug und der Verarbeitung der erhobenen Daten im SOC zum Zweck von Angriffserkennung und -management.

Nach dem Grundsatz von Privacy by Design (vgl. Art. 25) sollten bereits im Fahrzeug nur die Daten erfasst werden, die für die späteren Prozesse tatsächlich benötigt werden. Die Speicherung „überschießender" Daten auf Vorrat dürfte mindestens erhöhten Begründungsaufwand erfordern. Gleiches gilt für die (fortgesetzte) Speicherung entsprechender Daten im Fahrzeug nach Übermittlung in das SOC.[61]

Eine wichtige datenschutzrechtliche „Stellschraube" dürften die Intervalle sein, in denen entsprechende Daten aus dem Fahrzeug erhoben werden. Im Fall der Erhebung anlässlich eines Werkstattbesuchs (z. B. über die OBD-2-Schnittstelle) dürfte die Verarbeitung für Zwecke der Cybersecurity unter weniger strikten Voraussetzungen möglich sein als im Fall einer Erhebung von Fahrzeugdaten „over the air" (OtA) in regelmäßigen Abständen oder sogar im Wege einer Echtzeitüberwachung. Die Zulässigkeit letzterer dürfte u. a. vom Risiko und dessen Eintrittswahrscheinlichkeit abhängen, sodass eine zeitlich engmaschige Überwachung der Cybersecurity erleichtert sein dürfte, wo der Schutz von Leib und Leben in Rede steht bzw. entsprechende Gefahren besonders immanent sind.[62]

Im Rahmen der Auswertungsprozesse im SOC wird maßgeblich darauf zu achten sein, dass eine Datenauswertung streng nach dem *Need-to-Know*-Prinzip erfolgt. Datenzugriffe auf unterschiedliche Datenkategorien sind durch entsprechende Zugriffsberechtigungen abzusichern. Auswertungen sollten, soweit möglich, auf Basis anonymisierter bzw. pseudonymisierter Daten erfolgen. Der Zugriff auf Daten, die ein konkretes Fahrzeug individualisieren, sollte nur unter engen Voraussetzungen (z. B. Mehraugenprinzip und entsprechende Dokumentation) möglich sein. Bei der Ausgestaltung der Prozesse scheint es sinnvoll, sich an den für den Compliance-Bereich entwickelten Stufen-Konzepten zu orientieren.[63]

Soweit Daten ursprünglich für andere Zwecke erhoben wurden und mit den Daten im SOC zusammengeführt werden sollen, wäre die Nutzung im SOC an den Vorgaben des Art. 6 Abs. 4 bzw. den korrespondierenden Normen des BDSG zu messen (Zweckänderung).

2. Speichern und Löschen von Daten im SOC

Die zulässige Dauer der Datenspeicherung im SOC ist anhand einer Erforderlichkeitsbetrachtung zu bestimmen (vgl. Art. 17 Abs. 2 lit. a. bzw. Abs. 3 lit. e). Je nach Verarbeitungszweck und Ziel der Auswertungen können im Einzelfall kurze Speicherzyklen geboten sein. Andersherum kann eine längere Speicherung von z. B. mehreren Wochen, Monaten etc. dort statthaft sein, wo (nur) eine Langzeitbetrachtung entsprechende Analysen ermöglicht. Die Sensitivität der gespeicherten Daten (z. B. Standortdaten) wird bei der Betrachtung ebenso eine Rolle spielen. In jedem Fall sind besondere Schutzmaßnahmen zu ergreifen, soweit dies möglich ist (u. a. verschlüsselte Speicherung, Pseudonymisieren oder das „Sperren" von Daten).

3. Spezielle Verarbeitungsszenarien

Im Übrigen dürfte die Zulässigkeit der Verarbeitung im SOC ganz wesentlich von der Sensitivität der betroffenen Datenkategorien abhängen.

Die Verarbeitung von Positionsdaten im Fahrzeugumfeld wird oftmals kritisch bewertet.[64] Die Verarbeitung von Positionsdaten für Zwecke eines SIEM dürfte durchaus möglich sein,[65] im Ergebnis aber sicherlich Beschränkungen unterliegen. Entsprechende Daten sind soweit möglich frühzeitig zu anonymisieren oder zu pseudonymisieren (z. B. durch gezieltes „Blurring" von Standortdaten). Werden für entsprechende Zwecke Standortdaten, die dem TKG unterfallen, verarbeitet, sind die speziellen Voraussetzungen des TKG-Datenschutzes zu beachten (vgl. §§ 91 ff. TKG), was auch für andere dem TKG unterfallende Daten gilt.

Weitere Beschränkungen können sich aus der Personengruppe der betroffenen Datensubjekte ergeben. So dürften

60 Vgl. Artikel-29-Gruppe, Opinion 06/2014 zum „Berechtigten Interesse" nach Artikel 7 der Richtlinie 95/46/EC, 844/14/EN, WP 217 vom 9.4.2014, abrufbar unter https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (zuletzt abgerufen am 10.7.2020).

61 Dass Fahrzeughersteller auch Datenverarbeitungsprozesse im Fahrzeug bereits im Entwicklungsstadium datensparsam zu gestalten haben, dürfte sich mangels Verantwortlichenstellung nicht unmittelbar aus der DS-GVO ergeben, wird aber bisweilen so gesehen; vgl. zum Ganzen die Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA), 2016, 3.

62 So i. E. wohl auch *Simo/Waidner/Geminn,* in: Roßnagel/Hornung (Fn. 3), 331.

63 Vgl. hierzu auch den Vergleich zu „Network Security Monitoring" und „Fraud Detection" durch *Simo/Waidner/Geminn,* in: Roßnagel/Hornung (Fn. 3), 331 m. w. N.; zu Compliance-Maßnahmen im Beschäftigungsverhältnis *Zöll* in: Taeger/Gabel, DSGVO – BDSG, 3. Aufl. 2019, § 26 BDSG Rn. 71.

64 Vgl. ZD-Aktuell 2012, 03029: Unzulässige GPS-Ortung von Mietwagen.

65 In diese Richtung CNIL, Compliance Package zum Datenschutz in Connected Cars, 2018, 30: „storing data relating to instantaneous speed and to geolocation in separate databases"; abrufbar unter https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data (zuletzt abgerufen am 12.7.2020).

bei der Verarbeitung von Beschäftigtendaten für Zwecke des SIEM zusätzlich die Voraussetzungen gemäß § 26 BDSG bzw. individual- und/oder kollektivarbeitsrechtliche Restriktionen zu beachten sein.[66]

4. Verarbeitung zur Beseitigung des Risikos

Inwieweit die im SOC gespeicherten Daten nach Erkennen des Angriffs auch für die unmittelbare Beseitigung eines Risikos verarbeitet werden dürfen, hängt maßgeblich von den korrespondierenden Handlungspflichten des Herstellers ab (vgl. hierzu zuvor V.). Obliegt es dem Hersteller danach, z. B. konkrete Maßnahmen im Hinblick auf einzelne betroffene Fahrzeuge einzuleiten, dürfte eine personalisierte Auswertung und Verarbeitung von Daten im SOC zu diesem Zweck statthaft sein. Wie bereits zuvor beschrieben, sollen die damit zusammenhängenden (datenschutzrechtlichen) Fragen an dieser Stelle jedoch nicht weiter vertieft werden.

5. Organisatorische Maßnahmen

Daneben werden weitere Schritte erforderlich sein, um zu einer datenschutzkonformen Ausgestaltung eines SIEM-Prozesses zu gelangen.

Gemäß Art. 13 sind die Betroffenen über die entsprechende Verarbeitung ausreichend zu informieren. Gemäß Art. 5 Abs. 2 (Rechenschaftspflicht) wird eine umfassende Dokumentation der Prozesse nebst Zugriffs- und Berechtigungskonzepten, Dokumentation der Systemzugriffe, Verantwortlichkeiten und Entscheidungsprozesse sowie ein ausreichendes Datenspeicherungs- und Löschkonzept zwingend erforderlich werden.

Aufgrund der mit entsprechenden Prozessen verbundenen umfassenden Datenverarbeitung dürfte die Durchführung eines Privacy Impact Assessments gem. Art. 35 unumgänglich sein. Inwieweit zusätzlich die Konsultation der zuständigen Aufsichtsbehörde erforderlich wird, bleibt im Einzelfall zu prüfen.[67]

VIII. Fazit und Ausblick

Automobilhersteller stehen angesichts der wachsenden Cyber-Gefahren, dem hohen Zeitdruck bei der Umsetzung der neuen Regularien und den datenschutzrechtlichen Sanktionsrisiken vor großen Herausforderungen.

Aus datenschutzrechtlicher Sicht ist es misslich, dass die existierenden Regelungen zur Cybersicherheit im Fahrzeug bislang keinen klaren Rahmen für die datenschutzrechtliche Zulässigkeit entsprechender Prozesse abstecken. Weitere Klarstellungen im Rahmen der Implementierung der UNECE-Regelungen in Europäisches Recht wären wünschenswert.

Bis dahin sollten sich für SIEM-Prozesse auf Basis der existierenden Regelungen sinnvolle Lösungen entwickeln lassen, die mit den datenschutzrechtlichen Vorgaben in Einklang gebracht werden können.

Ein wesentlicher Erfolgsfaktor für Automobilhersteller wird darin liegen, die datenschutzrechtliche Betrachtung frühzeitig in die Projektplanung zu integrieren und mit der produkthaftungsrechtlichen Perspektive zu verschmelzen – damit der Datenschutz nicht zum „Showstopper", sondern zum „Selling Point" entsprechender Lösungen werden kann.

66 Vgl. UNECE-Regulierungsentwurf zur Vehicle Cybersecurity, Version vom 23.6.2020 (Fn. 12), Table A.1 und C.1, 19/38, in denen auf das Risiko sog. „Insider" (Innentäter) verwiesen wird und entsprechende Maßnahmen gefordert werden.

67 Vgl. Entwurf der kroatischen Ratspräsidentschaft vom 21.2.2020, ErwG 21 c (Fn. 13), der in diese Richtung deutet.

RA Dr. Till Naruisch, LL.M., Dipl.-Ing. Bernd Degen und Dipl.-Ing. Rainhold Labza, Frankfurt a. M./Rüsselsheim*

Die neue VO (EU) 2018/858 im Überblick – Herausforderungen für Compliance-Systeme von Automobilherstellern

Das regulatorische Umfeld für Automobilhersteller wird zunehmend schwieriger. Die neue VO (EU) 2018/858 reformiert den Rechtsrahmen für die EU-Typgenehmigung und ergänzt diesen um eine intensivierte bereichsspezifische Marktüberwachung. Fahrzeuge, die bereits auf dem Markt sind, sollen häufiger auf Konformität überprüft werden. Hersteller sind gut beraten, die neuen rechtlichen und organisatorischen Erfordernisse in ihre bestehenden Compliance-Systeme einzupflegen. Die rechtssichere organisatorische Ausgestaltung und die Befolgung des technischen Rechts haben hierbei oberste Priorität.

I. Hintergrund und Historie

Die neue VO (EU) 2018/858[1] (Rahmenverordnung) reformiert den Rechtsrahmen für die EU-Typgenehmigung von Fahrzeugen.[2] Ergänzt wird dieser durch die umfangreich geregelte bereichsspezifische Marktüberwachung von Fahrzeugen und Komponenten in der EU. Der neue Rechtsrahmen soll für mehr Qualität und Unabhängigkeit bei der Typgenehmigung und Prüfung von Fahrzeugen sorgen.

* Auf Seite III erfahren Sie mehr über die Autoren.

1 Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates vom 30.5.2018 über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge, zur Änderung der Verordnungen (EG) Nr. 715/2007 und (EG) Nr. 595/2009 und zur Aufhebung der Richtlinie 2007/46/EG.

2 Dieser Beitrag stellt die persönlichen Auffassungen der Autoren dar, die nicht notwendigerweise den Auffassungen ihrer Kanzlei oder ihres Unternehmens entsprechen.