Deloitte.

Automotive Cybersecurity

Krisen- und Notfallübungen für eine dauerhafte Resilienz

Executive Summary

Automotive Cybersecurity ist von entscheidender Bedeutung für den Schutz und die Sicherheit von Fahrern, Passagieren, Fahrzeugen und anderen Assets wie personenbezogenen Daten. Neben den physischen Risiken können auch rechtliche Folgen und Reputationsschäden für die Automobilindustrie eine Rolle spielen. Angesichts des zunehmenden Einsatzes von (digitaler) Technologie ist es für Automobilunternehmen immer wichtiger, sich der potenziellen Risiken bewusst zu sein und angemessene Kontrollmaßnahmen zu ergreifen.

Der rechtliche Rahmen

In der Europäischen Union wird der rechtliche Rahmen für Automotive Cybersecurity durch die UN-R 155 definiert. Diese Verordnung verpflichtet Automobilerstausstatter (sogenannte OEMs) und Zulieferer dazu, angemessene Prozesse zur Reaktion auf Sicherheitsvorfälle zu etablieren. Dies bedeutet, dass sie in der Lage sein müssen, schnell und effektiv auf Cyberangriffe zu reagieren und mögliche Schäden zu begrenzen. Eine solide und effektive Cybersecurity-Strategie ist somit nicht nur aus Sicherheitsgründen von Bedeutung, sondern auch, um rechtlichen Anforderungen zu entsprechen.

MAKING AN IMPACT THAT MATTERS since 1845

Die Bedeutung von Übungen
Die Corona-Pandemie hat gezeigt, dass viele Regierungen, Unternehmen und Einzelpersonen auf unvorhergesehene Notfälle unzureichend vorbereitet sind. Um dies zu vermeiden, sind regelmäßige Übungen entscheidend, um eine effektive Reaktion auf (Sicherheits-)Vorfälle sicherzustellen. Dies gilt auch für die Automobilindustrie. Durch wiederkehrende Testläufe können Unternehmen Vertrauen im Umgang mit Sicherheitsvorfällen aufbauen, ihre Stärken und Schwächen identifizieren, die Koordination verbessern, das Bewusstsein für Cybersecurity schärfen und ihre Resilienz stärken.

Unser Serviceportfolio
Wir bieten Automobilunternehmen umfangreiche Dienstleistungen aus einer Hand, um gemeinsam deren Fähigkeiten hinsichtlich Vorfallsmanagement und Resilienz auszubauen. Hierzu zählen Beratungsleistungen zur Erstellung von Prozessen und Organisationsstrukturen, Analyse und Optimierung von Abläufen sowie die Durchführung von Krisen- und Notfallübungen. Unser „Continuous Capability Building Methodology" ist ein wertvolles Programm, um Unternehmen langfristig in der Reaktion auf Vorfälle und im Krisenmanagement zu unterstützen. Wir helfen unseren Kunden aus der Automobilindustrie, sich optimal auf potenzielle Cyberangriffe und andere Sicherheitsvorfälle vorzubereiten, um deren Kunden und Fahrzeuge effektiv zu schützen.

Cybersecurity ist ein bedeutender Faktor für die Produktsicherheit und erfordert Aufmerksamkeit sowohl von Automobilherstellern als auch von Zulieferern. Um die Sicherheit von Fahrern, Passagieren, Fahrzeugen und anderen Vermögenswerten zu gewährleisten, sind die Einhaltung der UN-R 155 sowie die Vorbereitung auf Notfälle durch regelmäßige Übungen un-erlässlich. Als erfahrener und zuverlässiger Partner bieten wir Unterstützung und Beratung für Kunden in der Automobilindustrie an, um ein effektives Notfall- und Krisenmanagement sowie ganzheitliche Resilienz zu erreichen.

Warum Deloitte?
- Zu unseren Kunden in der Automobilindustrie gehören einige der weltweit größten OEMs, Zulieferer, Händler, firmeneigenen Finanzunternehmen und Aftermarket-Hersteller.
- Umfassende Erfahrung und Erkenntnisse aus implementierten UNECE-Readiness-Programmen und Best Practices sowie zertifiziertem CSMS inkl. Typgenehmigungen
- Standardisierter und integrierter Bewertungsansatz eingebettet in unser „Automotive Supplier Cybersecurity Framework" unter Berücksichtigung aktuell geltender Vorschriften und Standards
- Globales Netzwerk aus erfahrenen Auditoren und Automotive-Cybersecurity-Spezialisten
- Standardisierungsgruppen: Wir sind Mitglied im DIN AK11 (ISO/SAE 21434, Cybersecurity) und DIN AK12 (ISO/AWI 24089, SUMS)

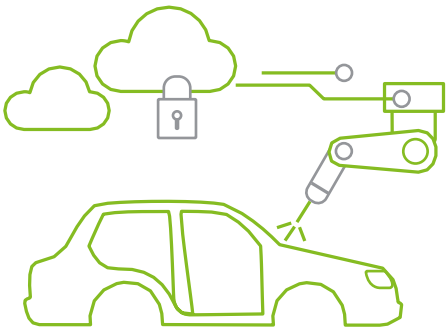
Cybersecurity ist eine „never ending story“

Die zunehmende Verwendung von vernetzten Technologien und Software erfordert immer robustere Cybersecurity-Maßnahmen. In diesem Artikel untersuchen wir deren Relevanz in der Automobilbranche und betrachten die rechtlichen Rahmenbedingungen. Wir zeigen auf, wie wichtig das Thema für die Unternehmensresilienz und das Krisenmanagement ist, insbesondere in Bezug auf Notfallreaktionen.

Warum ist Automotive Cybersecurity relevant?

In den letzten Jahren haben Risikobewertungen, Studien und unser -Engagement für unsere Kunden einen klaren Trend in Bezug auf Cyberbedrohungen aufgezeigt. Die steigende Zahl und Vielfalt von Bedrohungen haben direkte Auswirkungen auf die Automobilindustrie, insbesondere im Hinblick auf den Wandel zur E-Mobilität und die Produktion der Fahrzeuge. Laut ENISA zielen Angriffe zunehmend auf vernetzte Fahrzeugflotten ab, was katastrophale Folgen haben kann.[3]

Die fortschreitende Digitalisierung und der Einsatz modernster Technologien wie GPS, Bluetooth, Wi-Fi, integrierter Mobilfunk und Apps haben sowohl für Automobilhersteller als auch ihre Kunden zahlreiche Vorteile gebracht. Doch damit gehen auch neue Sicherheitsrisiken einher, die von Angreifern ausgenutzt werden und zu Diebstahl, Betrug, Datenschutzverletzungen oder sogar physischen Sicherheitsrisiken führen können. Ein einzelner Cyberangriff könnte beispielsweise Tausende Fahrzeuge gleichzeitig gefährden und das Risiko für die öffentliche Sicherheit erheblich erhöhen, wobei sich der Schaden möglicherweise sogar bis zum Hersteller ausbreiten kann.



93%
aller Automobilhersteller erlitten laut Forbes eine direkte Beeinträchtigung der Cybersecurity aufgrund von Schwachstellen in ihrer Lieferkette.[1]

66%
der Cyberangriffe konzentrierten sich laut ENISA (2021) auf den Lieferantencode.[2]

Die Automobilindustrie steht vor einer Vielzahl von Bedrohungen, darunter Infotainment-Bugs, gehackte Paywalls und kostenpflichtige Funktionen oder für die physische Sicherheit relevante Cyberangriffe auf Fahrzeuge.

[1] Chuck Brooks, MORE Alarming Cybersecurity Stats For 2021 ! (sic), Forbes, 24. Oktober 2021, abgerufen am 20. März 2023.
[2] European Union Agency for Cybersecurity, ENISA Threat Landscape For Supply Chain Attacks, Juli 2021, abgerufen am 20. März 2023.
[3] European Union Agency for Cybersecurity, ENISA Threat Landscape 2022, Oktober 2022, abgerufen am 20. März 2023.

Wie gestaltet sich der rechtliche Rahmen für Automotive Cybersecurity?
Die Europäische Union hat mit Inkrafttreten und Übernahme der UN-Regelung 155 eine Reihe von Anforderungen für Automobil-OEMs und -Zulieferer geschaffen, um Vorgehensweisen zur Reaktion auf Vorfälle einzuführen und umzusetzen. Dazu zählt auch die Notwendigkeit, Prozesse zur Erkennung und Reaktion auf Cybersecurityvorfälle zu etablieren, wie beispielsweise Pläne zur Reaktion auf Vorfälle und Notfälle sowie die Fähigkeit, solche Vorfälle zu erkennen und zu melden. Zusätzlich sollten Automobilhersteller und -zulieferer über ein „Incident Response Team" verfügen, eine klare Kommunikationsstrategie entwickeln und ihre Mitarbeiter durch theoretische und praktische Schulungen auf ihre Rolle und Verantwortung vorbereiten.

Welche exemplarischen Notfallszenarien und Auswirkungen sind von höchster Relevanz?
Die Automobilindustrie steht vor einer Vielzahl von Bedrohungen, darunter Infotainment-Bugs, gehackte Paywalls und kostenpflichtige Funktionen oder für die physische Sicherheit relevante Cyberangriffe auf Fahrzeuge. Einem Kollektiv von Forschern gelang es beispielsweise im Jahr 2022, durch Sicherheitslücken in vernetzten Fahrzeugen und Unternehmensplattformen, die sensible Daten enthalten, Zugriff auf Kundendokumente, Herstellerplattformen und interne Unternehmenskanäle zu erlangen.[4] Insgesamt sind mehr als 12 Millionen Fahrzeuge weltweit solchen und ähnlichen Risiken ausgesetzt. Die Auswirkungen eines Cyberangriffs können sowohl für Fahrzeugbesitzer als auch für OEMs schwerwiegend sein. Erstere können Opfer von Diebstahl, Betrug und weiteren Sicherheitsvorfällen werden. Für OEMs kann dies zu Schäden am Markenimage und potenziellem Vertrauensverlust der Kunden führen, was sich auch auf Beziehungen zu Investoren, Lieferanten und Produktionsnetzwerken sowie mögliche Joint Ventures für Forschungs- und Entwicklungszwecke auswirken kann. Auch Auftrags- und Umsatzrückgänge sind möglich. Darüber hinaus könnten OEMs für Schäden haftbar gemacht und zu entsprechenden Zahlungen verpflichtet werden, wenn ein Cyberangriff zu Schäden an Fahrern, Insassen oder ihrer Umgebung (Infrastruktur und Umstehende) führt.

- **Infotainment-Bugs**
  Da Fahrzeuge zunehmend vernetzt sind, ist das Infotainmentsystem zu einem beliebten Ziel für Cyberangreifer geworden. Bugs können von lästigen Störungen, die die Funktionalität des Systems beeinträchtigen und den Fahrer ablenken, bis hin zu schwerwiegenderen Sicherheitsverletzungen reichen, die die Privatsphäre des Fahrers und der anderen Fahrzeuginsassen gefährden.

- **Gehackte Paywalls und kostenpflichtige Funktionen**
  Ein weiteres mögliches Szenario ist das Hacken von Paywalls oder kostenpflichtigen Funktionen von Fahrzeugen, wodurch der Angreifer ohne Bezahlung auf das System oder Systeminhalte zugreifen könnte. Dies könnte zu erheblichen finanziellen Verlusten für den betroffenen OEM führen.

- **Datenschutzverletzungen**
  Cyberangreifer können sich Zugang zu sensiblen Daten verschaffen, die in vernetzten Fahrzeugen gespeichert sind, wie bspw. personenbezogenen oder finanziellen Daten, wodurch Halter oder Besitzer dem Risiko von Identitätsdiebstahl und anderen Formen der Cyberkriminalität ausgesetzt werden.

- **Für die physische Sicherheit relevante Cyberangriffe**
  Die gravierendste Art des Cyberangriffs betrifft die Sicherheitsfunktionen des Fahrzeugs und kann zu schwerwiegenden Schäden für Fahrer, Insassen oder Passanten führen. Ein Hacker könnte beispielsweise die Kontrolle über das Brems- oder Beschleunigungssystem oder die Lenkung des Fahrzeugs übernehmen und dadurch das Leben von Menschen und die Sicherheit der umliegenden Infrastruktur gefährden.

Wie beschrieben haben Cyberangriffe in der Automobilindustrie weitreichende und schwerwiegende Auswirkungen. Automobil-OEMs und -Zulieferer müssen proaktiv handeln, um sich vor diesen Bedrohungen zu schützen und die Sicherheit ihrer Kunden und Fahrzeuge zu gewährleisten.

Zwei wesentliche Elemente für eine effektive Reaktion auf Vorfälle sind:

- **Regelmäßige Notfallübungen**, bei denen ein simuliertes Notfallszenario entworfen und nachgestellt wird, um die Bereitschaft und Reaktionsfähigkeit des Reaktionsteams eines Unternehmens zu testen. Die Übungen werden in einer kontrollierten Umgebung durchgeführt, sodass das Team seine Aufgaben und Zuständigkeiten ohne das Risiko realer Konsequenzen üben kann.

- **Die Zusammenarbeit zwischen Automobilherstellern und -Zulieferern** ist ein wachsender Trend zur Bewältigung der gemeinsamen Herausforderungen im Bereich der Cybersecurity. Dazu gehören der Austausch von Informationen über Bedrohungen und Best Practices sowie die Teilnahme an gemeinsamen Übungen zur Reaktion auf Vorfälle. Außerdem hat es sich als vorteilhaft erwiesen, Prozesse anzugleichen und die Zusammenarbeit an kritischen Schnittstellen zu verbessern.

[4] Sam Curry, Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More, Blog, 03. Januar 2023, abgerufen am 20. März 2023.

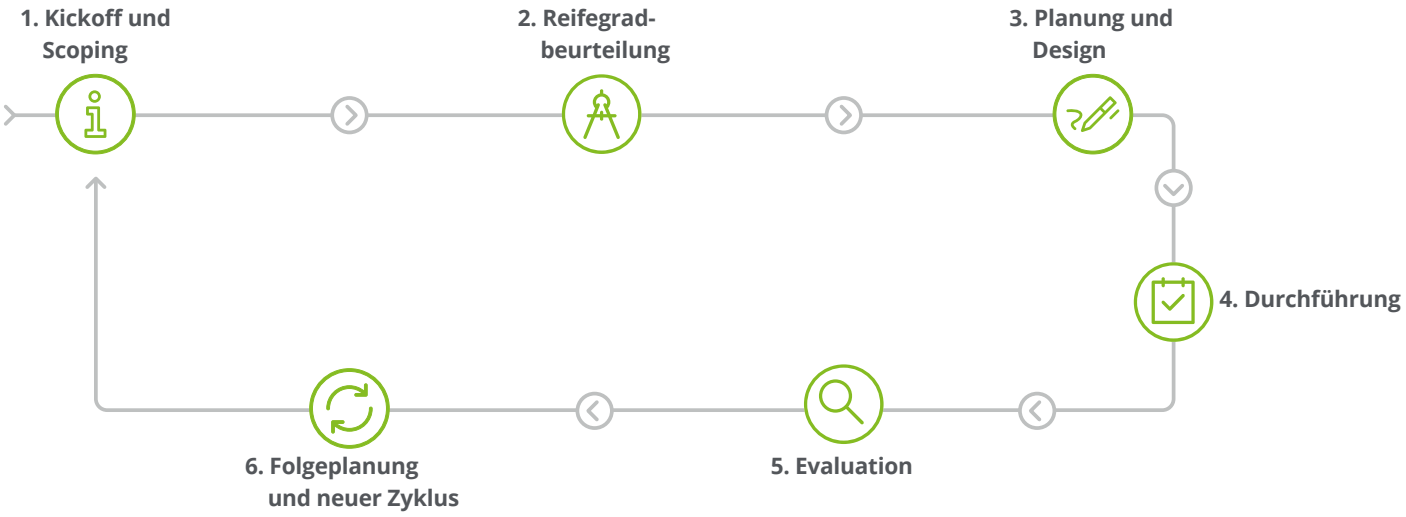
Welche Dienstleistungen bieten wir für Automobil-OEMs und -Zulieferer an?

Als zuverlässiger und kompetenter Partner in der Automobilbranche bieten wir umfassende Beratungsdienste für die Vorbereitung und Reaktion auf Cybersecurity-vorfälle an. Wir sind davon überzeugt, dass ein effektives Krisen- und Notfallmanagement einen ganzheitlichen Ansatz erfordert, der alle relevanten Stakeholder einbezieht und eine klare Kommunikationsstrategie für Kunden, Lieferanten und Mitarbeiter umfasst. Zu unseren Dienstleistungen gehören die Beratung zur Prozessgestaltung und Organisationsstruktur, die Analyse und Optimierung von Abläufen sowie die Vorbereitung und Durchführung von Krisen- und Notfallübungen. Darüber hinaus bieten wir theoretische und praktische Schulungsmaßnahmen an, um Führungskräfte und Mitarbeiter auf ihre Rollen und Verantwortlichkeiten innerhalb der Incident-Response-Organisation vorzubereiten. Durch gezielte Awareness-Maßnahmen vermitteln wir das Ziel und die Anforderungen des Vehicle-Security-Incident-Managements an eine breitere Mitarbeiterschaft.

Gemeinsam mit unseren Kunden entwickeln wir ein individuelles, realistisches und anspruchsvolles Szenario, basierend auf dem Reifegrad der vorhandenen Incident-Response-Organisation. Wir evaluieren relevante Übungsziele und erstellen ein Skript, das sogenannte „Injects“ beinhaltet, um das Response-Team herauszufordern, ohne es zu überfordern. Anschließend leiten wir Optimierungsmaßnahmen ab.

Unsere Spezialistinnen und Spezialisten verfügen über umfangreiche Erfahrungen in der Entwicklung, Durchführung und Analyse von Notfällen und gewährleisten einen szenariobasierten und daher realistischen Handlungsablauf der Testläufe. Wir berücksichtigen den Erfahrungsstand der Teilnehmer in Bezug auf bestehende Pläne, Prozesse und relevante Dokumentation, um die Qualität der Übung unabhängig von der Ausbildung auf taktischer oder strategischer Ebene sicherzustellen. Je nach Bedarf werden relevante Stakeholder und externe Parteien in verschiedene Übungsbereiche einbezogen, um einen realistischen Aufbau sicherzustellen und umsetzbare Erkenntnisse zu liefern.

Abb. 1 – „Continuous Capability Building Methodology“
Unsere Methodik kann als regelmäßiger Zyklus zum Auf- und Ausbau von Fähigkeiten beschrieben werden:



1. Kickoff und Scoping
- Etablieren eines gemeinsamen Verständnisses von Übungszielen, Rahmenbedingungen, Teilnehmern und Stakeholdern
- Vorstellen der Organisation, Strukturen und Prozesse des Incident-/Krisenmanagements

2. Bei Bedarf: Reifegradbeurteilung
- Etablieren eines gemeinsamen Verständnisses des Incident-Management-Frameworks und des Reifegrads
- Review der relevanten Dokumentation (z.B. Prozesse)
- Interviews mit Stakeholdern des Incident-Managements
- Empfehlungen für Übungen, die darauf abzielen, die Fähigkeiten zur Reaktion auf Vorfälle und die Resilienz der Organisation zu verbessern
- Entwerfen einer Roadmap für den langfristigen Auf- und Ausbau von Fähigkeiten (z.B. über die nächsten drei Jahre)

3. Planung und Design
- Gemeinsame Entwicklung und Gestaltung von Szenarien, Skripten und Einspielern (sog. Injects)
- Veranschaulichung von Alarmierungsstrukturen, einschließlich wichtiger Drittanbieter entlang der Lieferkette
- Festlegung von Bewertungskriterien auf der Grundlage des Reifegrads, der Übungsziele, regulatorischer Anforderungen und Best Practices
- Erstellung von Medieneinspielern mithilfe des Deloitte CrisisSimulator sowie von Unterlagen für die Übung
- Abstimmung des Kooperationsmodells (z.B. basiert das Kooperationsmodell von Deloitte auf FORDEC, einer Methode zur strukturierten Entscheidungsfindung aus der Luftfahrt)

4. Durchführung
- Der Moderator und die Übungskoordinatoren von uns werden die Reaktion des Response-Teams und die Maßnahmen zur Bewältigung des Vorfalls genau verfolgen.
- Das Szenario wird durch Injects eskaliert oder deeskaliert, um ein angemessenes Übungsniveau für die Teilnehmer zu gewährleisten.
- Die Übung wird in Zusammenarbeit zwischen uns, dem Moderator und mittels einer unterstützenden Struktur durchgeführt und durch Spezialisten aus der Kundenorganisation ergänzt.
- Es erfolgt unmittelbares Feedback für und von den Teilnehmern.

5. Evaluation

- Der Übungsbericht folgt einer klaren Struktur und dient als Nachweis für die Response- und Managementverfahren (sofern die Übungsziele erreicht werden).
- Basierend auf etablierten Methoden und Best Practices beurteilen und analysieren wir die Übungsergebnisse und schätzen die Performance der Teilnehmer ein.
- Abhängig von den identifizierten Lücken und Erkenntnissen werden klare, konkrete Maßnahmen zur Verbesserung abgeleitet.
- Nach Überprüfung, Feedback und abschließender Genehmigung durch die relevanten Stellen wird der Bericht finalisiert.

6. Folgeplanung und neuer Zyklus

- Planung und Entwurf eines Umsetzungsplans bzgl. der ausgearbeiteten Optimierungsmaßnahmen
- Review des durchlaufenen Übungs- und Optimierungszyklus und ggf. Anpassung der Projektzusammenarbeit
- Überprüfung der Roadmap (falls erforderlich) und gemeinsame Definition der Rahmenannahmen/Kriterien für die nächste Übung
- Planen des nächsten Kickoffs und der zukünftigen Ziele (z.B. gemäß Roadmap)

Warum sind regelmäßige Übungen entscheidend für ein effektives Notfall- und Krisenmanagement?

Es ist entscheidend, dass Unternehmen regelmäßig ihre Incident-Response-Fähigkeiten üben und verbessern, um im Ernstfall eine effektive Reaktion gewährleisten zu können. Hier einige der wichtigsten Vorteile regelmäßiger Übungen:

- **Vertrauensaufbau**
  Durch regelmäßige Teilnahme an Übungen entwickeln Organisationen und Mitarbeiter Routinen und Vertrauen in ihre Fähigkeit, wirksam auf Notfälle zu reagieren. Vertrauen in erlernte Fähigkeiten und etablierte Prozesse ist unerlässlich, um im Ernstfall effektiv handeln zu können.
- **Identifizierung von Stärken und Verbesserungsbereichen**
  Regelmäßige Notfallübungen bieten die Möglichkeit, Optimierungsbereiche in den Krisenmanagement- und Incident-Response-Prozessen oder -Strukturen eines Unternehmens zu identifizieren und zu adressieren. Gewonnene Erkenntnisse dienen langfristiger Fähigkeitenentwicklung, um auf eine sich ständig ändernde Bedrohungslandschaft zu reagieren. Ziel ist eine nachhaltige und kontinuierliche Entwicklung der unternehmerischen Resilienz.
- **Verbesserung der Koordination**
  Regelmäßige Übungen stärken die Koordination zwischen den verschiedenen am Reaktionsprozess beteiligten Stake-holdern, einschließlich Mitarbeitern, Lieferanten, Kunden und Aufsichtsbehör-den. Diese verbesserte Koordination ist entscheidend für eine effektive und effiziente Reaktion auf Notfallsituationen.
- **Awareness/Bewusstsein schärfen**
  Regelmäßige Response-Übungen schärfen das Bewusstsein für die Bedeutung des Krisenmanagements und die Rolle aller Beteiligten in der Reaktionsstruktur. Dieses erhöhte Bewusstsein ist entscheidend für eine schnelle und effektive Reaktion auf einen Notfall.

Fazit

In der sich ständig weiterentwickelnden Automobilindustrie wird die Stärkung der Cybersecurity zunehmend wichtiger, um neuen potenziellen Bedrohungen vorzubeugen. Geeignete Maßnahmen und Prozesse sind unerlässlich, um Cyberangriffe abzuwehren, die Sicherheit von Kunden zu gewährleisten und folglich die Reputation der Marke zu schützen.

Unser „Continuous Capability Building Methodology" ist ein wertvolles Programm für Unternehmen, die ihre Fähigkeiten zur Reaktion auf Vorfälle und ihr Krisenmanagement verbessern möchten. Durch die Simulation eines Vorfallszenarios in einer kontrollierten Umgebung können Organisationen ihre Reaktionsfähigkeit testen, Verbesserungsbereiche identifizieren und notwendige Änderungen vornehmen, um ihre Reaktionsprozesse kontinuierlich weiterzuentwickeln. Dadurch sind Unternehmen besser darauf vorbereitet, auf Notfälle zu reagieren und die Sicherheit ihrer Kunden und Vermögenswerte zu gewährleisten. Wir sind bestens gerüstet, um Automobil-OEMs und Zulieferer beim Erreichen dieser Ziele zu unterstützen.

Literaturverzeichnis

- Chuck Brooks, MORE Alarming Cybersecurity Stats For 2021 ! (sic), Forbes, 24. Oktober 2021, abgerufen am 20. März 2023.
- European Union Agency for Cybersecurity, ENISA Threat Landscape 2022, Oktober 2022, abgerufen am 20. März 2023.
- European Union Agency for Cybersecurity, ENISA Threat Landscape For Supply Chain Attacks, Juli 2021, abgerufen am 20. März 2023.
- Sam Curry, Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More, Blog, 03. Januar 2023, abgerufen am 20. März 2023.

Ihr Ansprechpartner

Michael Müller
Offering Lead Partner
Crisis & Resilience
Tel: +49 30 25468 5225
micmueller@deloitte.de

Ingo Dassow
Partner
Global Lead Automotive Cybersecurity
Tel: +49 30 25468 451
idassow@deloitte.de

Helge Wengerowski
Manager
Crisis & Resilience
Tel: +49 40 32080 4232
hwengerowski@deloitte.de

Deloitte.

Stand 04/2023