DICONIUM

Cybersicherheit in der Automobilindustrie

Studie unter 200 Automotive-Entscheider:innen in Deutschland

Q3 2025

Wegweiser durch die Studie

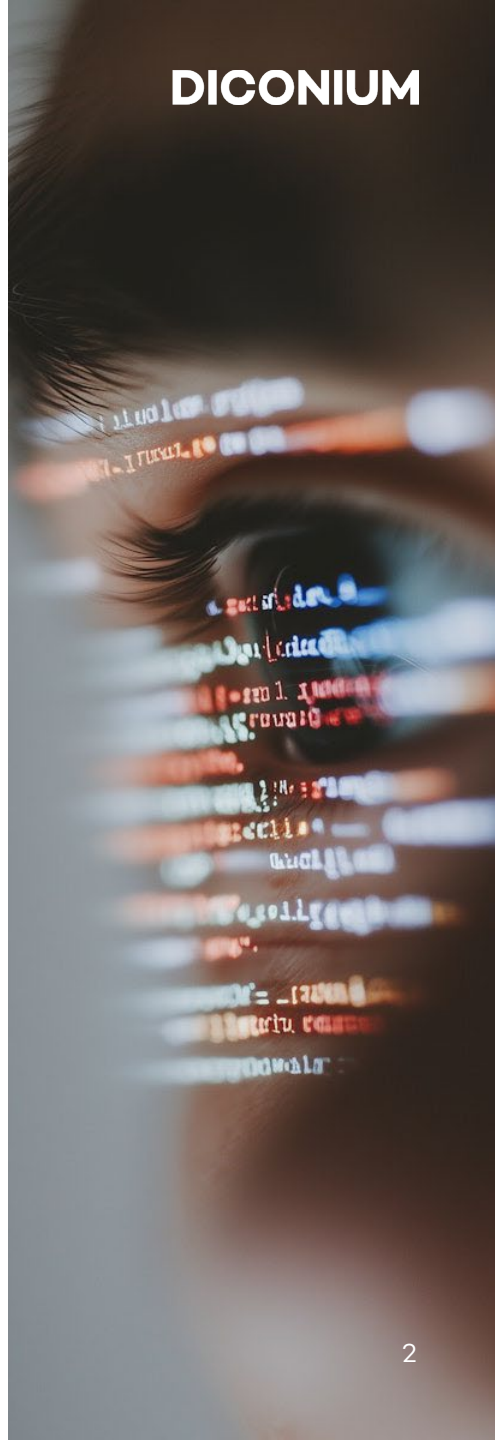
Die Automobilindustrie nimmt Cyberangriffe sehr ernst: Drei von vier Unternehmen (75%) schätzen die Gefahr durch Cyberangriffe als „hoch“ oder „sehr hoch“ ein.

Was die Branche in Sicherheitsfragen noch umtreibt, haben wir gemeinsam mit techconsult in einer Umfrage unter 200 IT-Entscheider:innen und Cybersicherheits-Expert:innen aus dem Automotive-Sektor herausgefunden.

Die Ergebnisse finden sich in dieser Studie.

techconsult TECHNOLOGY MARKET ANALYSTS | EIN UNTERNEHMEN DER heise group

DICONIUM



01 Die Automobilindustrie fühlt sich bedroht

Wie schätzen Sie die aktuelle Bedrohungslage im Bereich Cybersicherheit in der Automobilbranche ein?

Bedrohungslage	Total %	< 50 Mitarbeiter:innen	50 – 499 Mitarbeiter:innen	400 – 999 Mitarbeiter:innen	1000 + Mitarbeiter:innen
Sehr hoch	24,0%	21,4%	26,8%	22,4%	21,7%
Hoch	50,5%	35,7%	45,1%	62,1%	50,0%
Neutral	18,5%	28,6%	22,0%	10,3%	19,6%
Gering	6,0%	-	6,1%	5,2%	8,7%
Keine Bedrohung	0,5%	7,1%	-	-	-

Unser Takeaway

Das Bewusstsein der Bedrohungslage wächst mit der Unternehmensgröße. Denn: Bei größeren und großen Einheiten sind die Verantwortlichkeiten für Cybersecurity klar geregelt. Kleinere Unternehmen sollten das adaptieren.

02 Die Cloud gibt Anlass zur Sorge

Was war Ihre größte Herausforderung im Bereich Cybersicherheit in den letzten 12 Monaten?

Herausforderung	Total %	< 50 Mitarbeiter:innen	50 – 499 Mitarbeiter:innen	400 – 999 Mitarbeiter:innen	1000 + Mitarbeiter:innen
Ransomware-/Malware-Angriffe	19,0%	28,6%	12,2%	13,8%	34,8%
Schwachstellen in vernetzten Fahrzeugen	14,0%	14,3%	14,6%	15,5%	10,9%
Sicherheit in der Cloud und bei Remote-Arbeit	19,5%	7,1%	19,5%	29,3%	10,9%
Datenschutzverletzungen und Datenschutzvorfälle	16,5%	21,4%	19,5%	12,1%	15,2%
KI-basierte Bedrohungen	14,5%	14,3%	15,9%	15,5%	10,9%
Fachkräftemangel im Bereich Cybersicherheit	12,0%	7,1%	14,6%	10,3%	10,9%
Anforderungen an die Einhaltung gesetzlicher Vorschriften	4,0%	7,1%	3,7%	3,4%	4,3%
Sonstiges	0,5%	-	-	-	2,2%

Unser Takeaway

Die Cloud ist Basis des technischen Fortschritts in der Branche, aber das macht sie als Angriffsziel interessant. Die befragten Cybersecurity-Expert:innen sehen diese Bedrohungen, die hier sogar höher eingeschätzt werden als die sonst führenden Angriffe mit Ransom- und Malware.

Datenschutzverletzungen und -vorfälle rangieren in der Sorgenliste recht weit oben. Die Verantwortlichen sind sich offenbar bewusst darüber, dass sie ihre Hausaufgaben bei IT-Sicherheit und Datenschutz erledigen müssen.

03 Das Vertrauen in die eigene Resilienz ist gering

Wie zuversichtlich sind Sie, dass Ihr Unternehmen Cyberangriffe verhindern und darauf reagieren kann?

Zuversicht	Total %	< 50 Mitarbeiter:innen	50 – 499 Mitarbeiter:innen	400 – 999 Mitarbeiter:innen	1000 + Mitarbeiter:innen
Eher besorgt: Es bestehen erkennbare Schwachstellen im aktuellen Sicherheitskonzept.	19,0%	12,2%	13,8%	13,8%	34,8%
Unentschieden: Es sind Maßnahmen vorhanden, aber die tatsächliche Wirksamkeit ist schwer einzuschätzen.	44,5%	41,5%	50,0%	50,0%	47,8%
Eher zuversichtlich: Unsere Schutzmaßnahmen sind solide, aber es gibt noch Optimierungspotenzial.	28,0%	30,5%	27,6%	27,6%	21,7%
Sehr zuversichtlich: Wir verfügen über sehr umfassende Sicherheitsmaßnahmen sowie routinierte und erprobte Reaktionspläne.	6,0%	4,9%	6,9%	6,9%	6,5%

Unser Takeaway

Die Zuversicht in die eigenen Fähigkeiten, Angriffe auf Systeme und Infrastrukturen abwehren zu können, ist nicht sonderlich groß. Noch größer aber ist die Unsicherheit darüber. Das deutet auf Sicherheitsstrukturen hin, die nicht oder nicht regelmäßig auf ihre Widerstandsfähigkeit getestet werden. Penetrations- und Stresstests können hier helfen.

04 Engpässe im Bereich Cybersecurity

Was ist Ihre größte Ressourcenlücke im Bereich Cybersicherheit?

Ressourcenlücken	Total %	< 50 Mitarbeiter:innen	50 – 499 Mitarbeiter:innen	400 – 999 Mitarbeiter:innen	1000 + Mitarbeiter:innen
Mitarbeiter (Talent/Mitarbeiterzahl)	30,0%	42,9%	26,8%	25,9%	37,0%
Prozesse (Frameworks/Verfahren)	24,0%	35,7%	29,3%	25,9%	8,7%
Technologie (Tools/Infrastruktur)	32,0%	14,3%	36,6%	36,2%	23,9%
Budget/Finanzierung	13,5%	7,1%	7,3%	10,3%	30,4%
Weiß nicht	0,5%	-	-	1,7%	-

Unser Takeaway

Technologie und Mitarbeitende sind die entscheidenden Träger der Cybersecurity, da stimmen wir unbedingt zu. Aber wir müssen darüber hinaus auch über die Strategie sprechen. Dazu gehört auch eine Governance, die Datensicherheit berücksichtigt, Prozesse absichert und die eigenen Mitarbeitenden vor Angriffen und Fehlern schützt. Nur in dieser Kombination kann Cybersecurity ganzheitlich wirken.

05 EU-Gesetzgebung zeigt Wirkung

Der Cyber Resilience Act trat Ende 2024 in Kraft, die wichtigsten Verpflichtungen gelten ab Dezember 2027. Wie wirkt sich dies auf Ihre Geschäftsplanung aus?

Auswirkung	Total %	< 50 Mitarbeiter:innen	50 – 499 Mitarbeiter:innen	400 – 999 Mitarbeiter:innen	1000 + Mitarbeiter:innen
Sehr hohe Auswirkung	19,0%	28,6%	23,2%	10,3%	19,6%
Hohe Auswirkungen	44,5%	28,6%	41,5%	50,5%	47,8%
Mittlere Auswirkungen	28,0%	35,7%	30,5%	27,6%	21,7%
Wenig Auswirkungen	6,0%	7,1%	4,9%	6,9%	6,5%
Sehr wenig Auswirkungen	2,0%	-	-	3,4%	4,3%

Unser Takeaway

Der Cyber Resilience Act der EU verpflichtet Hersteller digitaler Produkte zu nachweisbarer Cybersicherheit über den gesamten Produktlebenszyklus hinweg. Dazu zählen auch vernetzte Fahrzeugkomponenten und Software. Die ab 2027 geltenden Vorschriften werfen schon jetzt ihre Schatten voraus: Unserer Umfrage zufolge ergeben sich klare Auswirkungen auf die Geschäftsplanung.

06 **Sichere Fahrzeuge und Risikomanagement sind priorisierte Investitionsbereiche**

Welche Cybersicherheitsbereiche haben für Sie in den nächsten 12–18 Monaten höchste Investitionsprioritäten?

Bereiche	Total %	< 50 Mitarbeiter:innen	50 – 499 Mitarbeiter:innen	400 – 999 Mitarbeiter:innen	1000 + Mitarbeiter:innen
Sichere Fahrzeugarchitektur und -design	19,0%	28,6%	33,3%	13,8%	30,4%
Bedrohungserkennung und Incident Response	14,0%	57,1%	40,7%	53,4%	45,7%
Lieferanten- und Drittanbieter-Risikomanagement	19,5%	-	35,8%	27,6%	32,6%
Einhaltung gesetzlicher Vorschriften (CRA, UNECE WP.29 usw.)	16,5%	28,6%	21,0%	44,8%	37,0%
KI-gestützte Sicherheitsanalysen	14,5%	28,6%	48,1%	36,2%	45,7%
Sicherheitsschulungen und Sensibilisierungsprogramme	12,0%	42,9%	30,9%	41,4%	26,1%
Sichere Over-the-Air (OTA)-Updatesysteme	4,0%	7,1%	24,7%	20,7%	17,4%
Schwachstellenmanagement und Penetrationstests	0,5%	14,3%	11,1%	3,4%	19,6%

Unser Takeaway

Die Branche hat verstanden, dass sie nachrüsten muss. Das ist eine, wenn nicht die wichtigste Erkenntnis der Umfrage. Und sie gilt nicht nur für die eigene Infrastruktur, sondern zu einem relevanten Teil auch für die eigenen Produkte. Gesetzliche und regulatorische Vorschriften mögen das beschleunigen, aber aus unserer Sicht ist das auch Ergebnis der wachsenden Aufmerksamkeit, die das Thema Cybersicherheit in der Branche genießt.

07 **Next Steps**

Wir haben unsere Schlüsse aus der Umfrage gezogen. Und Sie?

Warten Sie nicht, bis sich Ihr CIO oder CISO mit einer Agenda an Sicherheits- und Infrastrukturmaßnahmen bei Ihnen meldet. Werden Sie als Entscheider:in selbst aktiv!

Machen Sie Cybersicherheit zum zentralen Managementthema, zu dem technische Herausforderungen gehören, vor allem aber das Wahrnehmen von Verantwortung. Eine klare Strategie mit einer Governance, die Unternehmensassets und die Mitarbeitenden vor Angriffen und Fehlern schützt, ist dringend erforderlich.

Cybersicherheit gibt es nicht zum Nulltarif. Investitionen in Infrastruktur und Personal sind notwendig – gerade dann, wenn es Ihnen an Vertrauen in die eigene Resilienz fehlt. Besonders wichtig sind aus unserer Sicht Investitionen in Bedrohungserkennung, Incident Response und KI-gestützte Sicherheitslösungen.

Testen Sie Ihre Cybersicherheitsinfrastruktur regelmäßig auf Sicherheitslücken, etwa durch Penetrations- und Stresstests. Beziehen Sie Ihre Mitarbeitenden ein – mit Schulungen und regelmäßigen Übungen. Nur dann sind Sie wirklich auf Notfälle vorbereitet!

Begreifen Sie gesetzliche Anforderungen als Ansporn: EU-Gesetze wie der Cyber Resilience Act verpflichten Hersteller zu Cybersicherheit. Automotive-Unternehmen sollten sich proaktiv auf diese Anforderungen vorbereiten und in Cybersicherheit investieren.

Methodik und Durchführung

Die vorliegende Studie zum Thema Cybersicherheit im Automobilsektor wurde im Auftrag von Diconium als Online-Befragung durch die **techconsult GmbH**, einem renommierten Marktforschungs- und Analyseinstitut der heise Gruppe, durchgeführt.

Im dritten Quartal 2025 wurden insgesamt 200 Entscheider aus deutschen Unternehmen der Automobilindustrie befragt, darunter OEMs und Tier-1-Zulieferer. Die Stichprobe umfasste Unternehmen aller Größenklassen, wobei gezielt Führungskräfte und IT-Entscheider:innen mit Kompetenz und Verantwortung im Bereich Cybersicherheit angesprochen wurden. Die Ergebnisse sind repräsentativ für Entscheider:innen in Unternehmen des Automobilsektors in Deutschland.

techconsult TECHNOLOGY MARKET ANALYSTS | EIN UNTERNEHMEN DER heise group

Weiterführende Links

Cybersecurity Insights in unserem Tech Blog:

- Diconium Blog

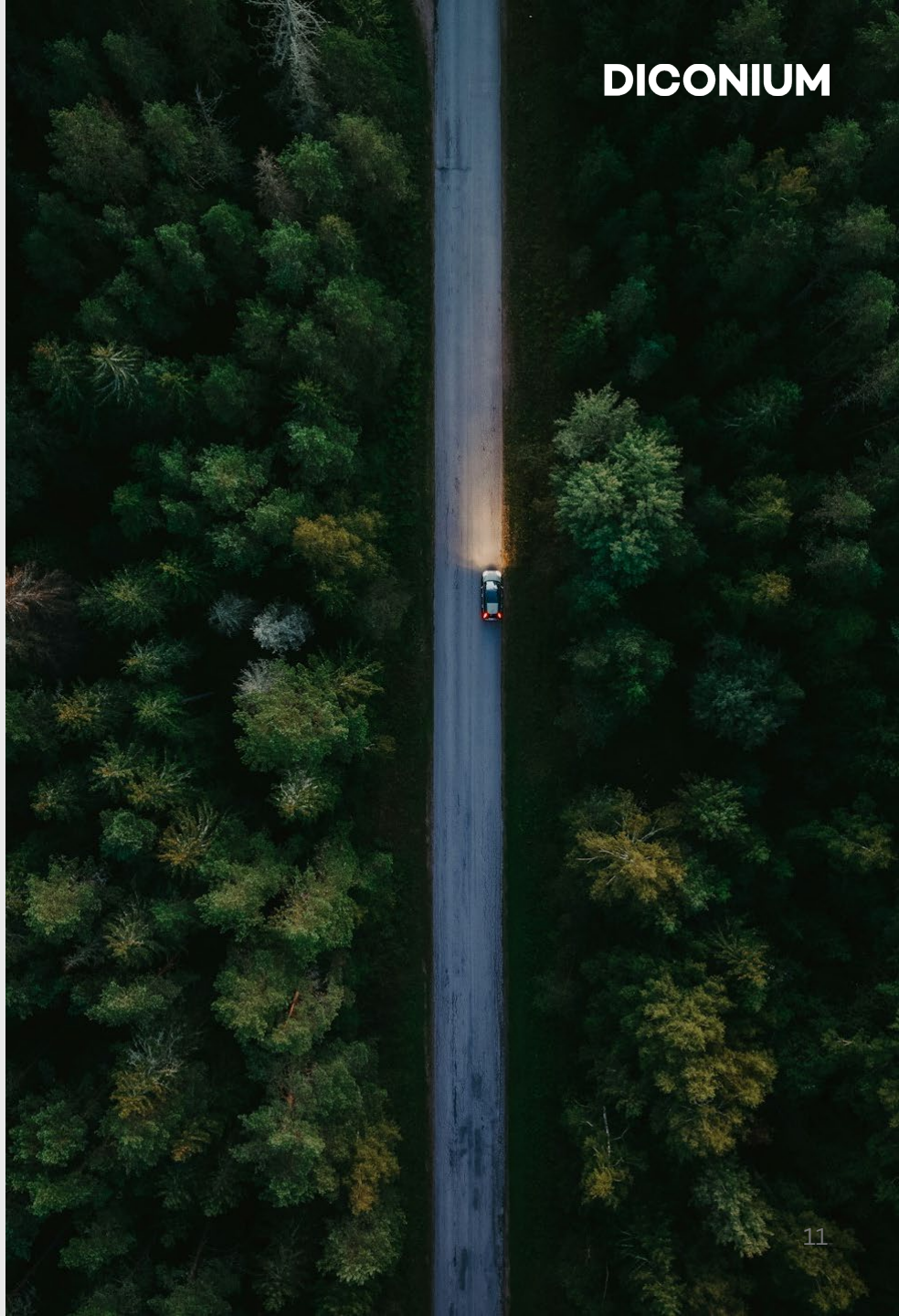
Cybersecurity Success Stories:

- Sichere IDS-Protokollierung für eine führende Automotive Software Division
- PKI-Lösung für einen führenden Automobilhersteller
- Trusted Application Development für einen Automobilzulieferer
- Cybersecurity Testing für Fernride

Diconium Cybersecurity Offerings:

Product Security, Software Security, IT Security, Security Infrastructure Services

Zur Übersicht



Über Diconium

Diconium ist Ihr Digital Business Transformation Partner – und das auf globalem Level. Wir meistern Komplexität und steigern die Wettbewerbsfähigkeit. Als hundertprozentige Tochter des Volkswagen-Konzerns leben wir digitale Exzellenz – im Automobilsektor, in der Industrie und darüber hinaus.

Mit 30 Jahren Transformationserfahrung in diversen Branchen sorgen wir dafür, dass digitale Innovationen durch Software, Daten und KI echten Mehrwert erzielen. Unsere Kunden sind multinationale Unternehmen aus verschiedenen Branchen, darunter Volkswagen, Stihl, Bechtle, Trumpf und Zeiss.

Mit Standorten in vier der fünf größten Volkswirtschaften der Welt – in Europa, Nordamerika und Asien – bringt unser diverses Team aus über 2.500 Expert:innen umfassende Expertise in den Bereichen Data & AI, Software Engineering, Integration & Testing, Cybersecurity und Digital Advisory ein. Mit unseren Lösungen stellen wir konventionelle Branchenstandards auf den Prüfstand und setzen neue Maßstäbe für digitale Spitzenleistung.

Bei allem, was wir tun, setzen wir uns dafür ein, Unternehmen aller Branchen und die Gesellschaft zu transformieren – für eine smartere, digitalere und lebenswertere Zukunft.

Weitere Informationen finden Sie auf www.diconium.com

DICONIUM

Bereit für mehr Sicherheit?
Schreiben Sie uns oder besuchen Sie uns online!

Schreiben Sie uns:
contact@diconium.com

Besuchen Sie uns:
diconium.com/de/offering/cybersecurity

We update industries and society –
building smart, digital, and desirable futures.