CLOUDFLARE

WHITEPAPER

Sicherheitsturbo: Was der Automobilbranche im Kampf gegen Cyberbedrohungen hilft

Sicherheitsturbo: Was der Automobilbranche im Kampf gegen Cyberbedrohungen hilft

Die Automobilindustrie, einst eine Bastion mechanischer Ingenieurskunst, steht heute, getrieben durch die zunehmende Vernetzung und das Aufkommen neuer Technologien, an vorderster Front der digitalen Revolution. Der Übergang von mechanischen zu digital vernetzten Systemen bringt neue Herausforderungen im Bereich der Cybersicherheit und des Datenschutzes mit sich. Fahrzeuge sind nicht mehr in erster Linie durch physischen Diebstahl gefährdet, sondern durch digitale Angriffe.

In den 1970er-Jahren waren Autos im Wesentlichen mechanische Konstruktionen, die kaum von dem beeinflusst waren, was heute als digitale Technik bezeichnet wird. Damals galt der physische Diebstahl als Hauptproblem: Einbrecher nutzten Techniken wie das Aufbrechen von Türschlössern oder das Überbrücken der Zündung, um ohne Schlüssel starten zu können. Neben der Verwendung falscher Schlüssel gehörten auch gewaltsame Überfälle zu den Bedrohungen. Mit dem Aufkommen digitaler Technologien in den 1980er- und 1990er-Jahren veränderte sich das Sicherheitsrisiko: Fahrzeuge avancierten zu vernetzten Systemen, die neue Angriffsflächen für Hacker boten. Die Bedrohung durch Cyberattacken nahm zu.

In den 2000er-Jahren rückten Cyberangriffe durch Hacker in den Mittelpunkt, waren aber noch nicht so weit entwickelt, industrialisiert und professionalisiert. Sicherheitsrisiken im Zusammenhang mit digitalen Angriffen zeichneten sich ab, steckten aber noch in den Kinderschuhen. Die 2010er-Jahre brachten einen weiteren Wandel: Schlüssellose Zugangssysteme und vernetzte Infotainment- und Telematiksysteme wurden zum Standard. Das Abfangen von Funksignalen und die Möglichkeit des Fernzugriffs auf Fahrzeuge entpuppten sich als neue Sicherheitsrisiken. Heute, in den 2020er-Jahren, erlebt die Automobilindustrie erneut eine rasante technologische Wandlung, an deren Spitze die Connected-Car-Technologien und die Software-defined Vehicle (SDV) stehen. Diese Innovationen verändern nicht nur die Art und Weise, wie Autos entwickelt und genutzt werden, sondern stellen die Entwickler auch vor neue Herausforderungen im Bereich der Cybersicherheit.

Warum eine umfassende Sicherheitsstrategie notwendig ist

Stellen Sie sich eine Welt vor, in der Hacker die Kontrolle über Ihr Fahrzeug übernehmen können, indem sie Bremsen, Lenkung und sogar die Motorleistung manipulieren. Dies ist keine ferne Science-Fiction, sondern eine reale Bedrohung, die ernsthafte Konsequenzen für die Sicherheit der Insassen und signifikante wirtschaftliche Schäden für Automobilhersteller und die gesamte Branche mit sich bringt. In den verborgenen Ecken der digitalen Welt, wo unsichtbare Technologienetzwerke unseren Alltag durchdringen, wird ein scheinbar unscheinbares Element wie das Rücklicht eines Autos zu einem kritischen Zugangspunkt. Es öffnet die Tür zum Controller Area Network (CAN-Bus) des Fahrzeugs, das bei Missbrauch die gesamte Fahrzeugfunktionalität gefährden kann.

In dieser zunehmend vernetzten Welt sind die Angriffsvektoren vielfältig und komplex. Zu den potenziellen Einfallstoren für solche Angriffe gehören nicht nur offensichtliche Schnittstellen wie Bluetooth und Wi-Fi, sondern auch weniger beachtete Punkte wie On-Board-Diagnose-Ports und sogar die Firmware-Updates der Fahrzeuge. Einmal im System, können Hacker Schwachstellen in der Software ausnutzen, um Kontrollbefehle an verschiedene Fahrzeugkomponenten zu senden. Solche Angriffsmuster reichen von einfachen Störungen (etwa das unerwartete Aktivieren des Scheibenwischers) bis hin zu tiefen Eingriffen in die Fahrzeugsteuerung.

Die Komplexität von Angriffen auf Autos ist sehr unterschiedlich und äußert sich in verschiedenen Aspekten. Einerseits können einige Angriffe automatisiert aus der Ferne erfolgen, und zwar ohne physischen Zugang zum Fahrzeug. Andererseits gibt es Szenarien, die einen physischen Zugang erfordern, um den Wagen zu kompromittieren. Diese Unterschiede in der Ausführung zeigen die Bandbreite der Bedrohungen, denen Automobile ausgesetzt sein können. Darüber hinaus konzentrieren sich Angriffe sowohl auf einzelne Fahrzeuge als auch auf ganze Fahrzeugflotten. Dies weist auf die Notwendigkeit hin, nicht nur einzelne Fahrzeuge zu sichern, sondern auch die gesamte Flotteninfrastruktur vor potenziellen Bedrohungen zu schützen.

Eine wichtige Rolle spielt auch der Ort des Angriffs, der vielfältig sein kann und sich über verschiedene Phasen der Fahrzeugnutzung und -herstellung erstreckt. Angriffe können in der Werkstatt während der Wartung erfolgen, indem sie Sicherheitslücken in Diagnosesoftware oder Hardware ausnutzen. Sie können aber auch bereits in der Produktionsphase beim Hersteller durch Eingriffe in den Produktionsprozess oder in die Softwareentwicklung erfolgen. Selbst auf der Ebene von Teilkomponenten wie Chips oder anderen kritischen Bauteilen sind Attacken möglich.

Ganzheitlicher Ansatz

Angesichts dieser Risiken ist es von entscheidender Bedeutung, dass alle Akteure entlang der Wertschöpfungskette – von den Automobilherstellern über die Zulieferer bis hin zu den Softwareentwicklern – ein tiefes Verständnis für potenzielle Sicherheitslücken entwickeln. Sie müssen proaktive Maßnahmen ergreifen, um diese Risiken zu minimieren. Ein ganzheitlicher Ansatz erfordert deshalb eine enge Zusammenarbeit aller Beteiligten, um einheitliche Sicherheitsstandards und -protokolle entlang der gesamten Kette zu implementieren und kontinuierlich aufrechtzuerhalten.

Im Mittelpunkt steht dabei die Umsetzung einer ganzheitlichen Sicherheitsstrategie, die sowohl die Hardware- als auch die Softwareebene umfasst. Diese Strategie sollte sich flexibel an die sich ständig ändernden Cyberbedrohungen anpassen lassen. Dazu gehören regelmäßige Sicherheitsüberprüfungen, die Aktualisierung der Schutzmaßnahmen und die kontinuierliche Schulung der Beschäftigten, um das Sicherheitsbewusstsein und die Sicherheitskompetenz zu stärken. Darüber hinaus ist es wichtig, robuste Notfallreaktionspläne für den Fall eines erfolgreichen Cyberangriffs zu entwickeln und umzusetzen. Die schnelle Identifizierung und Behebung von Sicherheitslücken sowie die Minimierung potenzieller Schäden stehen dabei im Mittelpunkt. Wenn jeder Teilnehmer der Wertschöpfungskette seine Verantwortung wahrnimmt und proaktiv handelt, gewährleistet das ein hohes Maß an Sicherheit und Vertrauen in die zunehmend vernetzte und digitalisierte Automobilindustrie.

Organisatorische Compliance

Um die vielschichtigen Anforderungen an die Fahrzeugsicherheit zu erfüllen, ist es unerlässlich, sowohl organisatorische als auch regulatorische Compliance sicherzustellen. Dies umfasst auf organisatorischer Ebene die Einhaltung interner und externer Vorschriften, Standards und Best Practices, die für die Automotive-Cybersicherheit von besonderer Relevanz sind. Der Fokus liegt darauf, dass sowohl Automobilhersteller als auch Zulieferer die gesetzlichen Anforderungen an Datenschutz und Datensicherheit erfüllen und gleichzeitig Best Practices und Richtlinien wie ISO 27001 oder IEC 62443 befolgen. Diese Standards minimieren die Sicherheitsrisiken in vernetzten Fahrzeugen.

Die Etablierung eines umfassenden Compliance-Programms fördert zudem eine Kultur der Cybersicherheit, sensibilisiert die Angestellten und reduziert das Risiko menschlicher Fehler. Regelmäßige Audits und Überprüfungen helfen dabei, Sicherheitsrichtlinien einzuhalten und an neue Bedrohungen anzupassen. Es ist wichtig, auch Lieferanten und Partner in die Compliance-Strategien einzubeziehen, um einheitliche Sicherheitsstandards entlang der gesamten Wertschöpfungskette zu gewährleisten. Dies stärkt das Vertrauen der Kunden und trägt zum Erfolg der Branche bei.

Regulatorische Compliance

Die regulatorische Compliance konzentriert sich besonders auf die Einhaltung der gesetzlichen Anforderungen an die Sicherheit vernetzter Fahrzeuge. Hier spielt die UNECE (United Nations Economic Commission for Europe) eine zentrale Rolle bei der Festlegung globaler Standards, wobei die UN-Regelung Nr. 155 die Sicherheitsanforderungen für autonome Fahrzeuge festlegt. Die EU-Richtlinie zur Cybersicherheit im Automobilsektor ergänzt diese Standards und stellt sicher, dass in der EU verkaufte Fahrzeuge die notwendigen Sicherheitsanforderungen erfüllen.

Diese internationalen und regionalen Vorschriften schützen die öffentliche Sicherheit und ermöglichen den internationalen Handel mit Fahrzeugen. Regelmäßige Sicherheitsbewertungen und -prüfungen gewährleisten die Einhaltung der aktuellen Sicherheitsstandards, fördern das Vertrauen der Verbraucher und unterstützen die Entwicklung innovativer, sicherer Automotive-Cybersecurity-Lösungen.

Wichtige Normen und Regelungen

ISO 27001

Bei ISO 27001 handelt es sich um eine Norm für Informationssicherheits-Management, die Anforderungen und Best Practices festlegt. In der Automobilindustrie schützt sie sensible Informationen und erfüllt hohe Standards.

IEC 62443

IEC 62443 ist eine internationale Normenreihe für industrielle Netzwerksicherheit, die Standards und Leitlinien für den Schutz von Automatisierungssystemen und industriellen Kontrollsystemen (ICS) definiert.

UNECE/ UN-Regelung Nr. 155

Die UNECE (Wirtschaftskommission für Europa der Vereinten Nationen) entwickelt internationale Standards für Fahrzeuge und Verkehrssicherheit. UN-Regelung Nr. 155 beschäftigt sich mit Sicherheitsanforderungen für autonome Fahrzeuge.

Reibungslose Kooperation in der Automobil-Wertschöpfungskette

Die komplexe Wertschöpfungskette der Automobilindustrie benötigt eine reibungslose Zusammenarbeit. Dies erfordert eine präzise Abstimmung und effiziente Kommunikation zwischen allen Beteiligten – von den OEM-Herstellern über die Zulieferer bis hin zu allen Akteuren des automobilen Aftermarkets (Ersatzteilmarkt inklusive Handel und Werkstätten). Die Integration von Sicherheitsstandards von Anfang an, regelmäßige Sicherheitsüberprüfungen sowie gezielte Schulungen zur Sensibilisierung für Sicherheitsrisiken spielen in diesem Gefüge eine zentrale Rolle. Nur die strikte Einhaltung geltender Compliance-Regeln und -Standards gewährleistet eine umfassende Cybersicherheitsstrategie.

Die Bedeutung von Investitionen in die Cybersicherheit innerhalb einer Wertschöpfungskette kann nicht hoch genug eingeschätzt werden. Solche Investitionen haben nicht nur einen direkten Einfluss auf das eigene Unternehmen, sondern wirken sich auf alle Akteure in der Kette aus. Das Konzept der „Schwachstelle in der Kette“ verdeutlicht, dass die Stabilität einer Wertschöpfungskette nur so stark ist wie ihr schwächstes Glied. Investitionen in die Cyberabwehr wirken wie eine starke Verteidigungslinie, während fehlende Investitionen diese Linie schwächen. Wenn ein Unternehmen in der Wertschöpfungskette die Cybersicherheit vernachlässigt, können Angreifer genau diese Schwachstelle ausnutzen, um die gesamte Kette anzugreifen. Das erhöht auch die Kosten und Risiken für alle anderen Firmen. Deshalb kommt der ganzheitlichen Betrachtung der Cybersicherheit entlang der Wertschöpfungskette eine zentrale Rolle zu.

Das Automobil-Ökosystem setzt sich aus zahlreichen Akteuren zusammen: Automobilhersteller, Zulieferer, Dienstleister, Regulierungsbehörden und Endnutzer. Automobilhersteller sind für die Fahrzeugentwicklung und die Integration von Technologien verantwortlich, während Zulieferer die notwendigen Komponenten bis hin zur Werkstatt liefern. Dienstleister bieten umfassende Vernetzungs- und Softwarelösungen an. Regulierungsbehörden legen Standards und Gesetze fest, während die Endnutzer die Fahrzeuge bewegen.

Im Kontext der Cybersicherheit umfasst die Wertschöpfungskette verschiedene Elemente, darunter Cybersicherheits-Stacks, die aus Hardware, Software, Services, Unified Threat Management, Vulnerability Management, Application Security, Managed Security Services sowie Risk and Compliance bestehen. Die Integration und effektive Koordination dieser Elemente bietet einen umfassenden Schutz vor Cybersicherheitsbedrohungen und trägt zur Sicherung des gesamten automobilen Ökosystems bei.

Welche Handlungsempfehlungen und Ansätze sinnvoll sind

Die Anforderungen an die Cybersicherheit steigen in der sich schnell entwickelnden Automobilindustrie immer mehr. Fahrzeuge verändern sich von Transportmitteln zu einem Teil unseres digitalen Lebens, wodurch der Schutz von Daten und Systemen eine wichtigere Rolle spielt. Erfolgreiche Unternehmen benötigen eine dynamische Cybersicherheitsstrategie, die technische Innovationen und kontinuierliche Weiterbildung umfasst. Chief Information Officers (CIOs) und Chief Information Security Officers (CISOs) gelten als Schlüsselakteure in diesem Prozess. Ihre Aufgabe besteht darin, technologischen Fortschritt und Datensicherheit in Einklang zu bringen und die branchenweite Zusammenarbeit bei der Entwicklung gemeinsamer Sicherheitsstandards zu fördern. Es folgen einige ausgewählte Empfehlungen.

1) V2X-Kommunikationstechnologien: Innovationen und deren Absicherung

Wichtig für Automobilhersteller: Sie müssen sicherstellen, dass V2X-Systeme (V2X: Vehicle-to-Everything-Kommunikation) widerstandsfähig gegen Cyberangriffe sind, während Datenschutz und -sicherheit gewahrt bleiben.

Beispiel & Empfehlung: Ein OEM (Original Equipment Manufacturer) integriert End-to-End-Verschlüsselung in die V2X-Kommunikation seiner Fahrzeuge.
CISOs sollten regelmäßige Penetrationstests und Sicherheitsbewertungen durchführen, um Schwachstellen vor der Markteinführung zu identifizieren und zu beheben.

2) Multilayered Security Approach: Mehrschichtige Verteidigungsstrategien

Wichtig für Zulieferer: Entwicklung eines mehrschichtigen Sicherheitskonzepts, das verschiedene Verteidigungslinien umfasst.

Beispiel & Empfehlung: Ein Zulieferer für Fahrzeugteile setzt Intrusion-Detection-Systeme und regelmäßige Sicherheitsupdates ein. CISOs sollten ein Framework für Incident Response und Recovery-Pläne entwickeln, um auf Sicherheitsvorfälle schnell reagieren zu können.

3) Sicherheits- und Datenschutzherausforderungen in der Fertigung

Wichtig für Fertigungsbetriebe: Implementierung effektiver Datenschutz- und Sicherheitsmaßnahmen in der Produktionskette.

Beispiel & Empfehlung: Ein Hersteller von Fahrzeugkomponenten führt Sicherheitsschulungen für Mitarbeiter durch und verwendet sichere Cloud-Technologien für die Speicherung sensibler Daten. CISOs sollten regelmäßige Audits zur Überprüfung der Einhaltung von Datenschutzrichtlinien durchführen.

4) OTA-Updates: Sicherheit in der Softwarewartung

Softwareentwickler in der Automobilindustrie müssen sicherstellen, dass OTA-Software-Updates (OTA: Over The Air) sicher und zuverlässig ablaufen.

Beispiel & Empfehlung: Ein Softwarelieferant für vernetzte Fahrzeuge implementiert mehrstufige Authentifizierungsverfahren für OTA-Updates. CIOs sollten in robuste Überwachungssysteme investieren, denn das gewährleistet die Integrität der Software während des gesamten Update-Prozesses.

5) SASE- und Zero-Trust-Modelle: Fortschrittliche Sicherheitskonzepte

Essenziell für IT-Abteilungen in der Automobilbranche: Einführung von dynamischen Zugangskontrollen und umfassende Überprüfung jeder Verbindung.

Beispiel & Empfehlung: Ein Fahrzeughersteller implementiert Zero-Trust-Sicherheitsmodelle für den Zugriff auf das interne Netzwerk. CISOs sollten ein konstantes Monitoring und eine dynamische Anpassung der Sicherheitsrichtlinien sicherstellen.

6) Die Rolle von IT- und Sicherheitsexperten: Proaktive Risikominderung

Automobilunternehmen sollten ein kompetentes Team zur kontinuierlichen Anpassung an neue Bedrohungen aufbauen.

Beispiel & Empfehlung: Ein Automobilzulieferer etabliert ein Cybersicherheitsteam, das sich auf die Entwicklung innovativer Sicherheitslösungen konzentriert. CIOs und CISOs sollten in die kontinuierliche Weiterbildung und Entwicklung ihrer Teams investieren.

7) Integration von Cybersicherheit in die Lieferkette

Wichtig für die gesamte Wertschöpfungskette: Verankerung eines Sicherheitsbewusstseins in allen Bereichen der Lieferkette.

Beispiel & Empfehlung: Ein Logistikunternehmen für Automobilkomponenten implementiert strengere Sicherheitsprotokolle für den Datenaustausch zwischen Lieferanten und Herstellern. CISOs sollten Sicherheitsaudits entlang der gesamten Lieferkette fördern, um Schwachstellen zu identifizieren und zu beheben.

8) Compliance und Einhaltung von Datenschutzgesetzen

Handlungsbedarf bei internationalen Automobilunternehmen: Sicherstellung der Einhaltung globaler Datenschutzgesetze und -normen.

Beispiel & Empfehlung: Ein multinationaler Automobilkonzern passt seine Datenschutzstrategien regelmäßig an internationale Standards an. CISOs sollten ein engagiertes Team für die Überwachung der Einhaltung von Datenschutzgesetzen etablieren.

9) Partnerschaften für gemeinsame Sicherheitsinitiativen

Kleinere Zulieferer und Start-ups sollten Kooperationen mit größeren Unternehmen aufbauen, um gemeinsame Sicherheitsstandards zu entwickeln.

Beispiel & Empfehlung: Ein Start-up im Bereich autonomes Fahren arbeitet eng mit etablierten OEMs zusammen, das hilft bei der Entwicklung von Sicherheitsprotokollen. CIOs und CISOs sollten das Wissen und die Ressourcen großer Partner nutzen, um Sicherheitsinitiativen gemeinsam voranzutreiben.

Was Cloudflare im Bereich Netzwerksicherheit und Datenschutz für die Automotive-Branche tun kann

Cloudflare hat sich als führender Anbieter für Netzwerksicherheit und Cybersecurity als unverzichtbarer Partner der vernetzten Automobilindustrie etabliert. Mit seiner fortschrittlichen Technologie und umfangreichen Erfahrung bietet Cloudflare maßgeschneiderte Lösungen, die sowohl die Online-Präsenz als auch die Netzwerkeffizienz und -sicherheit für Unternehmen in dieser Branche optimieren. Das spielt eine entscheidende Rolle in einer immer vernetzteren Welt, in der die Anforderungen an die Leistungsfähigkeit und Sicherheit der Systeme ständig steigen.

Doch was bedeutet das für die Zulieferer, die die Produktion und Lieferung von Fahrzeugkomponenten verantworten? Für sie ist die Integration in das Cloudflare-Netzwerk von unschätzbarem Wert. Mit Lösungen wie Firewall-as-a-Service sorgt Cloudflare dafür, dass die Kommunikation und der Datenaustausch zwischen Zulieferern und Herstellern sicher und zuverlässig ablaufen. Dies garantiert Effizienz und Sicherheit in der gesamten Lieferkette.

Auch Autohändler und Werkstätten stehen vor der Herausforderung, sich sicher mit den zentralen Systemen der Hersteller zu verbinden. Cloudflare ermöglicht ihnen dies auf gefahrlose und effiziente Weise. Insbesondere für den sicheren Empfang und die Durchführung von Over-the-Air-Updates spielen solche Netzwerkdienste eine zentrale Rolle. Und die Endnutzer? Obwohl sie nicht direkt mit Cloudflare interagieren, profitieren sie indirekt von den verbesserten Sicherheits- und Netzwerkdiensten, die Cloudflare für OEMs und Zulieferer bereitstellt. Ein geschützteres und effizienteres Netzwerk führt zu einem besseren Nutzererlebnis und zu zuverlässigeren Diensten.

Insgesamt bietet Cloudflare eine Plattform, die die Bedürfnisse aller Akteure in der Automobilindustrie berücksichtigt und unterstützt. Von der Optimierung der Online-Präsenz über die Verbesserung der Netzwerkeffizienz bis hin zur Gewährleistung der Sicherheit: Cloudflare optimiert die Leistungsfähigkeit und Sicherheit von Systemen in der vernetzten Automobilindustrie.

Fazit

Für Führungskräfte in der Automobilindustrie ist es von entscheidender Bedeutung, sich kontinuierlich an die Herausforderungen der Cybersicherheit anzupassen. Mit der zunehmenden Bedeutung vernetzter Fahrzeuge müssen sie verstärkt auf innovative Sicherheitsmechanismen und robuste Datenschutzmaßnahmen setzen. Die Kombination aus fortschrittlicher Technologie, regelmäßigen Mitarbeiterschulungen und Teamwork steht im Zentrum bei der Entwicklung effektiver Sicherheitsstrategien. Die Auswahl eines führenden und visionären Dienstleisters und Kompetenzträgers ist unabdingbar. Durch die ständige Anpassung an neue Bedrohungslandschaften und die Einhaltung internationaler Datenschutzstandards können Führungskräfte nicht nur die Sicherheit erhöhen, sondern auch die Wettbewerbsfähigkeit stärken und das Vertrauen der Kunden sichern.

Über Cloudflare

Cloudflare, Inc. (NYSE: NET) ist der führende Anbieter im Bereich der Connectivity Cloud. Als Unternehmen versetzt Cloudflare Organisationen in die Lage, ihre Mitarbeitenden, Anwendungen und Netzwerke überall schneller und sicherer zu machen und gleichzeitig Komplexität und Kosten zu reduzieren. Aufbauend auf einem der größten und am besten vernetzten Netzwerke der Welt blockiert Cloudflare für seine Kunden täglich Milliarden von Online-Bedrohungen.

Kontaktadresse:

Cloudflare Germany GmbH
Rosental 7, 80331 München

Kontakt:

Telefon: +49 (89) 26207202
E-Mail: enterprise@cloudflare.com
https://www.cloudflare.com/de-de