VARGROUP

[8.974 Zeichen inkl. Leerzeichen]

Automobilbranche: Cybersicherheit ist nicht mehr optional

Wie Vehicle Security Operations Center (VSOC) Fahrzeuge virtuell absichern

Ein Mausklick – und der Motor geht aus. Plötzlich bleiben Tausende Fahrzeuge stehen, andere fahren in sie hinein, Menschen werden verletzt. Was wie ein Szenario aus einem Science-Fiction-Film klingt, ist längst reale Bedrohung. Bereits 2015 haben es Sicherheitsforscher mit dem berühmten Jeep-Cherokee-Fall [siehe Infobox] bewiesen: Sie übernahmen mit einem Laptop aus mehreren Kilometern Entfernung die Kontrolle und manövrierten den Geländewagen in einen Graben. Auch wenn die Automobilbranche seitdem dazugelernt hat: Sicherheitslücken bestehen heute immer noch und werden sogar immer gravierender – denn die Fahrzeuge werden zunehmend vernetzter.

Zwar wird Cybersicherheit innerhalb der Automobilbranche immer intensiver diskutiert – doch auf dem Markt fehlt oft noch das Bewusstsein für ihre Bedeutung. Dabei stellt sich nicht länger die Frage „ob“, sondern „wann“ ein Cyberangriff stattfinden wird. Viele Unternehmen haben dennoch keine effektive Cybersicherheitsstrategie und das, obwohl mit fortschreitender technischer Entwicklung das Risiko für Cyberangriffe rapide steigt. Diese Diskrepanz hat den Gesetzgeber auf den Plan gerufen: Mit der neuen EU-Bestimmung UN R155, die seit Juli 2024 gilt, ist Cybersicherheit für neue Fahrzeuge Pflicht. Laut dieser Richtlinie müssen Autohersteller und Zulieferer ein Cyber Security Management System (CSMS) nachweisen. Sie müssen in der Lage sein, Sicherheitsvorfälle im Auto festzustellen, Angriffe aus der Ferne zu erkennen und abzuwehren – und das über die gesamte Fahrzeuglebensdauer hinweg. Damit benötigt die Automobilbranche ein geeignetes System, wie es in der IT schon lange etabliert ist: ein Security Operations Center (SOC), doch in spezieller Ausführung für die Anforderungen der Automobilbrache – also ein Vehicle Security Operations Center, kurz: VSOC.

VSOC – Cyberschutz für die Automobilbranche

VSOC ist ein spezialisiertes Sicherheitszentrum, das sich auf die Überwachung und Erkennung von sowie die Reaktion auf Cyberbedrohungen konzentriert, die speziell Fahrzeuge betreffen. Es ist keine neue Erfindung. Im Prinzip gleicht es einem SOC, das in der klassischen IT die gleichen Funktionen übernimmt: eine permanente Fernüberwachung sehr vieler Parameter, um Anomalien automatisiert zu erkennen und bei Bedrohungen Alarm zu schlagen. Cybersecurity wird also nicht gewährleistet, indem Hackerangriffe vollständig verhindert werden – das ist in vernetzten Systemen nicht möglich – sondern indem man Bedrohungen systematisch frühzeitig erkennt und rechtzeitig Gegenmaßnahmen einleitet, um die Schäden zu minimieren. Dazu überwachen in einem

Kontrollzentrum IT-Sicherheitsexperten Prozesse und Protokolle und reagieren auf eintretende Sicherheitsvorfälle, sogenannte Incidents. Bei der Flut ständig entstehender Daten gleicht diese Arbeit der Suche nach der Stecknadel im Heuhaufen – und wäre ohne KI, maschinelles Lernen und automatisierte Überwachungsprozesse nicht zu leisten. Mit ihrer Hilfe kann das SOC-Personal aus den vielen Ereignissen, die von normalen Vorgängen abweichen, die wesentlichen herausfiltern und sich auf diese echten Incidents konzentrieren. Doch wenn es diese Technologien schon gibt, weshalb benötigt die Automobilbranche dann überhaupt spezialisierte VSOCs?

Auch wenn beide Systeme auf dem gleichen Prinzip beruhen, unterscheiden sich das Know-how, die Prozesse und ihre Gegebenheiten. Während sich ein klassisches SOC um Bedrohungen für IT-Netzwerke und Unternehmenssysteme wie Server und Computer kümmert, hat das VSOC-Personal mit Angriffen auf fahrzeugspezifische Komponenten zu tun. Dazu gehören zum Beispiel eingebettete E/E-Systeme, Türsteuergeräte, Fahrerassistenzsysteme, Fahrwerksteuerung oder fahrzeuginterne Kommunikationssysteme. Dementsprechend unterscheiden sich die Angriffsvektoren: In der IT sind es beispielsweise Phishing-Mails und Malware; im Automobilsektor sind es unter anderem Denial-of-Service-Attacken, bei denen Kommunikationskanäle mit dem Ziel der Funktionsstörung oder gar des Ausfalls angegriffen werden, oder Remote Code Execution, wobei zum Beispiel Schwachstellen im Infotainmentsystem ausgenutzt werden, um schädliche Codes einzuspielen und Kontrolle über Fahrzeugfunktionen zu erlangen. Entsprechend schwerwiegender sind die Auswirkungen im Automotive-Sektor, die schnell lebensbedrohlich werden können – sowohl für die Autoinsassen selbst als auch für andere Verkehrsteilnehmer. Dramatisch wird es, wenn dabei nicht nur einzelne Fahrzeuge infiziert werden, sondern beispielsweise über eine E-Ladesäule Schadcodes in alle dort aufladenden Autos eingespielt und erst nach einiger Zeit aktiviert werden.

Eine zentrale Rolle bei Cyberangriffen spielt deshalb die Reaktionszeit auf Sicherheitsvorfälle. Je schneller das Risiko erkannt wird, desto schneller können Maßnahmen (der „Incident Response“) eingeleitet werden. Dabei unterscheiden sich SOC und VSOC aufgrund der technischen Infrastruktur stark voneinander: In der klassischen IT ist die übliche Vorgehensweise zur Behebung von Sicherheitslücken das Einspielen von Software-Updates – binnen Minuten umsetzbar über das Netz oder einen Server. Im Automobilbereich ist dieser Prozess wesentlich komplizierter, die Reaktionszeiten deutlich länger. Zwar können Updates moderne Fahrzeuge „over-the-air“, also über die Cloud, erreichen, doch oft hat der Hersteller gar nicht den Zugriff auf die Soft- und Hardware-Komponenten seiner Zulieferer, den diese aus nachvollziehbaren Gründen nicht offenlegen möchten. Deshalb müssen in diesem Fall die Fahrzeughersteller mit dem jeweiligen Lieferanten zusammenarbeiten, um eine Lösung zu finden – teilweise über mehrstufige Lieferketten hinweg. Und nicht jedes „embedded system“ kann per Remote-Update erreicht werden, sodass Rückrufe nötig werden. Je nach Länge der Kommunikationswege kann es Wochen dauern, bis eine Sicherheitslücke behoben wird. Im Extremfall müssen Hersteller die Fahrzeugbesitzer dazu aufrufen, ihre Autos vorläufig nicht mehr zu benutzen, oder sie legen die Fahrzeuge zwangsweise still – ein Alptraum für Halter und Hersteller.

Darüber hinaus unterscheidet sich der Umgang mit Threat Intelligence, also dem Know-how über mögliche Cyberbedrohungen. In einem “normalen” SOC werden die Bedrohungsdaten aus bereits erfolgten Cyberangriffen üblicherweise innerhalb der Branche geteilt und veröffentlicht, um die Abwehr global zu verbessern – ist eine Sicherheitslücke oder ein Exploit einmal bekannt, kann sie schneller wieder erkannt werden. Das beschleunigt die Abwehrprozesse und dient allen. Diese IT-Threat Intelligence kann nicht einfach auf die Automobilbranche übertragen werden. Denn einerseits fehlt der fahrzeugspezifische Kontext wie etwa die jeweiligen Komponenten. Andererseits widerspricht dem der Datenschutz: Von Fahrzeugen – und damit deren Haltern – produzierte Daten sind vertraulich und dürfen deshalb nicht beliebig verteilt werden. Deshalb sind Incident Responses bei einem VSOC komplizierter und erfordern spezielles Know-how. Außerdem sind die Fahrzeughersteller oft nicht bereit, negative Erfahrungen mit dem Wettbewerb und der Öffentlichkeit zu teilen – zu groß ist die Angst vor Wettbewerbsnachteilen und einem Imageschaden.

Zukunft sichern

Moderne Fahrzeuge verfügen bereits heute über 100 Millionen Codezeilen – eine Boeing 787 MAX dagegen lediglich über 15 Millionen[1]. Die Frage der Cybersicherheit ist somit längst nicht mehr nur eine Angelegenheit der IT-Branche. Wenn ein SOC auch grundlegende IT-Sicherheitsaufgaben übernehmen kann, ist doch ein speziell auf den Automobilsektor ausgerichtetes VSOC entscheidend, um eine effiziente Cyberabwehr zu garantieren. Angesichts der zunehmenden Fahrzeugkomplexität sollten Autohersteller das Thema Cybersicherheit proaktiv angehen und umfassende Maßnahmen ergreifen, um die Sicherheit ihrer Kunden zu gewährleisten und das Vertrauen der Verbraucher zu stärken. Es ist wichtig, dass sie über die bloße Einhaltung gesetzlicher Vorgaben hinausgehen und Cybersicherheit als eine zentrale Herausforderung betrachten, die es zu meistern gilt. Einige Hersteller haben den Handlungsbedarf bereits erkannt und nutzen die bereits vorhandenen Technologien, um innovative Sicherheitslösungen zu implementieren.

Der Autor, Werner Schimanofsky wird am 22.10.2024 im Rahmen des Messeauftritts von Yarix, Geschäftsbereich Cybersicherheit der Var Group, auf der it-sa 2024 einen Vortrag zum Thema „The importance of IT- and Product Cybersecurity for a holistic BCM approach“ im Knowledge Forum D um 16.45 Uhr halten. Am Yarix-Stand in Halle 7A, Stand 7A-106 können sich MessebesucherInnen umfassend über die Sicherheitslösungen SOC und VSOC informieren. Yarix-SicherheitsexpertInnen stehen Interessierten gerne persönlich für offene Fragen zu diesen und weiteren Themen zur Verfügung.

Zusatzinformation: Infoboxen

[850 Zeichen inkl. Leerzeichen]

Der Wandel zum IoT-Device auf Rädern

[1] https://www.vda.de/de/themen/digitalisierung/automatisiertes-fahren

Die starke Digitalisierung und Personalisierungswünsche der Autofahrer machen Fahrzeuge zunehmend zu IoT(Internet-of-Things)-Devices auf Rädern: Das Handy verbindet sich automatisch mit dem HotSpot im Auto, dank dem Zugriff auf das Smartphone wird die Spotify-Playlist abgespielt und freie Parkplätze am Zielort werden direkt auf dem Infotainment-Bildschirm angezeigt. Diese Funktionen in modernen Fahrzeugen erfordern Vernetzung: mit anderen Fahrzeugen, Infrastruktur, Anbieter-Cloud und anderem – das Auto ist fester Bestandteil von IoT-Infrastruktur. Stündlich erzeugt ein fahrendes KFZ bis zu 25 Gigabyte Daten, die leicht abgefangen werden können, einschließlich Informationen zum Fahrer und den Passagieren. Das Konzept des Connected Car öffnet Hackern neue Tore – und das, obwohl die bestehenden nicht einmal geschlossen wurden.

[1290 Zeichen inkl. Leerzeichen]

Der Jeep-Cherokee-Fall

Charlie Miller und Chris Valasek sind IT-Sicherheitsforscher und führen Cyberattacken auf Fahrzeuge durch, um die Sicherheitslücken aufzudecken und gleichzeitig die Automobilindustrie auf die Cybergefahren aufmerksam zu machen. 2015 haben sie in den USA über das Uconnect-Infotainmentsystem eines Jeep Cherokee Kontrolle über Türverriegelung, Klimaanlage, Scheibenwischer, Bremsen, Beschleunigung und im Rückwärtsgang sogar über das Lenkrad übernommen. Das Uconnect ist mit dem Internet verbunden und besitzt demnach eine IP-Adresse, also eine Zahlenfolge, über welche es sich digital „adressieren“ lässt - das war der Zugang für Miller und Vasalek aus der Ferne. Auch wenn das System nicht direkt mit dem CAN-Bus, also dem Kommunikationsnetzwerk zwischen fahrzeuginternen elektronischen Steuergeräten, verbunden ist, war es den Forschern möglich, vom Infotainmentsystem über die Diagnose-Schnittstelle die Kommunikation zum Bus-System herzustellen. Ursprünglich wurde diese Schnittstelle so programmiert, dass sie die CAN-Bus-Signale nur empfangen und selbst keine senden kann. Doch da das Bus-System ein kleiner Computer ist, lässt es sich umprogrammieren – so gelang es den beiden, die Kommunikation zu Steuergeräten aufzubauen und gänzlich die Kontrolle über das Auto zu übernehmen.

[706 Zeichen inkl. Leerzeichen]

Wer greift Autos an?

Cyberkriminelle haben unterschiedliche Beweggründe. Manche wollen Profit schlagen, andere sind politisch motiviert. Mit sogenannter Ransomware legen kriminelle Gruppen Autos still, drohen damit oder greifen sensible Daten ab, um Lösegeld (engl.: Ransom) von Herstellern oder Flottenbetreibern zu erpressen. Cyberattacken werden auch zu Terrorzwecken ausgeübt, der Begriff hierfür heißt Cyber-Terrorismus. Sie haben beispielsweise zum Ziel, möglichst viele Menschen zu verletzen oder die Wirtschaft nachhaltig zu schwächen. Auch bei Hacktivismus stehen politische Interessen im Vordergrund: Das Wort vereint Hacking und Aktivismus. Szenarien wie das Lahmlegen mehrerer Fahrzeuge aus Gründen des Klimaschutzes sind in diesem Kontext denkbar.

Die Var Group ist ein internationaler Anbieter digitaler Dienstleistungen und IT-Lösungen. Seit mehr als 50 Jahren unterstützt die Var Group Unternehmen jeder Größe bei der digitalen Evolution. Dabei liegt der Fokus auf Smart Services, Digital Cloud, Digital Security, Multimedia Workspaces, Data Science, Digital Experience, VarIndustries, Business Application International, Industry Solution Retail & Logistik in der Food-Branche. Als 360° IT-Dienstleister – von Beratung und Strategie über Implementierung bis Service und Wartung – bedient das Unternehmen den industriellen Sektor in Branchen wie Automotive, Maschinenbau, produzierendes Gewerbe, Pharma, Lebensmittel, Textilien, Mode, Luxus und Möbel sowie den Einzelhandel.

Die Var Group S.p.A. mit Sitz in Empoli (Italien) und einem Jahresumsatz von 823 Mio. Euro ist der italienische Marktführer für Software- und Systemintegrationslösungen und über ihre Muttergesellschaft Sesa an der italienischen Börse notiert. Über 3.850 hochqualifizierte Mitarbeitende in 13 Ländern unterstützen Kunden dabei, sich erfolgreich für den Wettbewerb in der Zukunft aufzustellen. Auf dem deutschen Markt agiert die Var Group durch ihre Tochter Var Group GmbH mit Sitz in München.

Als Mitglied des UN Global Compact setzt sich der IT-Spezialist aktiv für Nachhaltigkeit und soziale Gerechtigkeit ein. Die Var Group verfolgt einen integrativen Ansatz und fördert Individualität, Vielfalt und Chancengleichheit, u. a. mit Programmen zur Förderung von Frauen in der IT-Branche und in Führungspositionen.

Weitere Informationen unter www.vargroup.de

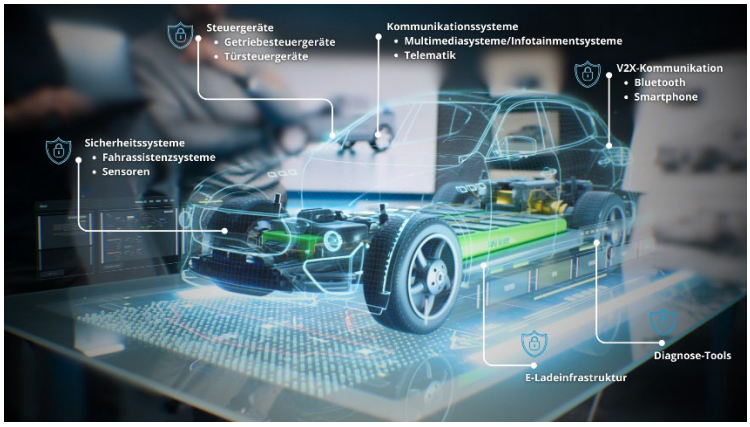
[Bilder und Text zur freien Verwendung]

Bildmaterial

[Autor_Werner_Schimanofsky]

Bildunterschrift: Autor: Werner Schimanofsky, Associate Partner & Head of Business Development for Automotive Cybersecurity bei CYRES Consulting, Business Unit der Var Group Deutschland | Foto: Var Group

[Schaubild_Angriffsvektoren_Connected_Cars]



Bildunterschrift: Von eingebetteten E/E-Systemen über Infotainment-Komponenten, Fahrerassistenzsysteme und Fahrwerksteuerung bis hin zu CAN-Bus: Moderne Autos bieten Hackern unterschiedliche Angriffsvektoren | Foto: Var Group

Pressekontakt

Volker Bischoff

Carta GmbH
www.carta.eu
Iggelheimer Straße 26
67346 Speyer
Deutschland

Mail: var@carta.eu
Tel.: +49 (0) 6232 / 100 111-22

Unternehmenskontakt

Franziska Unterfrauner

Var Group
www.vargroup.de
Mies-van-der-Rohe-Straße 8
80807 München
Deutschland

VARGROUP

Mail: f.unterfrauner@vargroup.com
Tel.: +49 (0) 1512 5021562