VW Das Werk

Treffen der Käferfreunde

In der Autostadt gibt es am Samstag einen Korso der Oldtimer und zwei Vorträge.

Wolfsburg. Am Samstag, 7. Mai, folgen rund 80 Besitzerinnen und Besitzer des Volkswagen Typs 1 dem Aufruf des 1. Käfer Clubs Wolfsburg und treffen sich ab 11 Uhr in der Autostadt von VW.

Die Volkswagen Osnabrück GmbH, Volkswagen Classic, die Stiftung Automuseum Volkswagen und auch die Autostadt präsentieren besondere Modelle aus den eigenen Sammlungen. Vor dem Treffen starten alle Teilnehmenden um 10 Uhr zu einem Korso durch Wolfsburg. In Vorsfelde beginnend, verläuft die Route über die Dieselstraße entlang des Berliner Rings über die Heinrich-Heine- und die Heinrich-Nordhoff-Straße, bevor es über die Berliner Brücke in die Autostadt geht.

Der Korso ist Höhepunkt des Treffens. FOTO: LEITZKE / AUTOSTADT

Zusätzlich gibt es laut Autostadt zwei Talkrunden rund um den Volkswagen Typ 1. Um 11.30 Uhr geht's auf dem Piazza-Vorplatz um das faszinierende Restaurationsprojekt eines 1303 Cabrios, und um 14.30 Uhr hält Dieter Landenberger, der Leiter Volkswagen Heritage, einen Vortrag im Volkswagen-Pavillon. Thema: „Wer hat's erfunden? – Die Entwicklungsgeschichte des Volkswagens". *red*

Besucher können das VW-Werk wieder besuchen

Nach zweijähriger Pause gibt es das beliebte Angebot auch als „Intensiv-Tour".

Wolfsburg. Nach zwei Jahren sind Werktouren im Wolfsburger VW-Stammwerk ab sofort wieder möglich. Das teilte der Autobauer jetzt mit.

Aufgrund der Corona-Auflagen hatte das Unternehmen die Führungen in Wolfsburg vorübergehend ausgesetzt – doch ab sofort können alle Gäste die Produktion der Wolfsburger Modelle wieder aus nächster Nähe erleben. Angefangen vom Presswerk mit der Straße 500, einer der größten Pressenstraßen im Konzern, über den Karosseriebau geht es in die Lackiererei und schließlich in die Montage zur sogenannten Hochzeit.

Werkleiter Rainer Fessel nahm mit dem gesamten Werkmanagement direkt an einer Tour teil und kommentierte in einer VW-Mitteilung hinterher: „Ich freue mich, endlich wieder Gäste und größere Gruppen aus der ganzen Welt in unseren Produktionshallen anzutreffen. Denn hier bei uns kann man den gesamten Fertigungsprozess erkunden. Das ist ein echtes Erlebnis für die ganze Familie." Giuseppe Lazzara, Leiter der Guest Relations, wird so zitiert: „Endlich geht es wieder los. Zwischenzeitlich war es ausschließlich nur virtuell möglich, sich die Produktion anzusehen. Wir haben ein super positives Feedback auf unsere virtuelle Werktour bekommen, welche auch weiterhin Bestand haben wird. Doch die zahlreichen Anfragen zeigen auch, dass sich sowohl unsere Kunden als auch unsere Kolleginnen und Kollegen danach sehnen, endlich wieder live vor Ort zu sein. Sie wollen erleben, wie ihr Fahrzeug entsteht und sie freuen sich auf spannende Themen wie Digitalisierung und Elektromobilität."

Während der vergangenen zwei Jahre hat das Team der Guest Relations an verschiedenen Projekten gearbeitet, um an Volkswagen Interessierten Alternativen anzubieten, sich weiterhin die Produktion anzusehen. Dabei ist unter anderem das Format „Faszination Produktion" für die Fahrzeugabholer im Themenkino der Autostadt entstanden. Auch von zu Hause aus können Gäste täglich an virtuellen Werktouren teilnehmen, die von Mitarbeitenden der Guest Relations moderiert werden. *red*

Reservierungen sind per E-Mail an werktour@volkswagen.de möglich. Die Werktour „Intensiv" ist kostenpflichtig (10 Euro für Erwachsene und 5 Euro ermäßigt) und dauert 60 bis 90 Minuten. Start und Ende der Werktour „Intensiv" ist am Tor 17. Einzelbuchungen können für dienstags um 14.15 Uhr und donnerstags um 10.15 Uhr angenommen werden. Gruppenbuchungen sind an Produktionstagen von Montag bis Freitag möglich.

Nach zwei Jahren Coronapause freuen sich die Mitglieder des Werktouren-Teams auf die Besucher der VW-Produktion. FOTO: DETLEV WECKE/VOLKSWAGEN AG

Cyberkriminelle können enorme wirtschaftliche Schäden anrichten. Und im Bereich der Automobilität geht es sogar um die Sicherheit der Fahrer und Insassen. Gerade autonom agierende Fahrzeuge könnten zum Ziel von Hackern werden. FOTO: FRANK RUMPENHORST / PICTURE ALLIANCE / DPA

Attacke auf VW – so wird ein Cyberangriff aufs Auto abgewehrt

Experten des VW-Partnerunternehmens Cymotive geben Einblicke in die Gefahrenlage.

Von Thomas Kruse

Wolfsburg. Ohne viel Aufhebens davon zu machen, hat Volkswagen vor einigen Jahren ein Partnerunternehmen gegründet. Cymotive ist so etwas wie die Lebensversicherung der Wolfsburger für ein neues Zeitalter der Mobilität. Wenn Autos autonom fahren – und das soll bereits in vier Jahren der Fall sein – dann bieten sie zugleich auch viel Angriffsflächen für manipulative Eingriffe von Hackern. Die können verheerende Folgen haben.

„Es wird höchste Zeit für Automobilhersteller und Zulieferer, über die traditionelle, funktionale Sicherheit hinauszudenken und neben der Safety verstärkt in Cybersecurity zu investieren. Denn es ist nur eine Frage der Zeit, bis wir ernsthafte, bösartige Cyberangriffe auf vernetzte Fahrzeuge sehen werden. Intrusion Detection Systeme (IDS) und Schwachstellenmanagement sind wichtige Maßnahmen, um Autos über ihren gesamten Lebenszyklus hinweg abzusichern", heißt es dazu in einer Pressemitteilung von Cymotive. Dass das eher im Stillen operierende Unternehmen nun verstärkt Öffentlichkeitsarbeit betreibt, hat damit zu tun, dass die Vorbehalte der Kundinnen und Kunden gegenüber autonom fahrenden Autos wohl noch größer sind als die gegenüber Elektroautos.

Für Wolfsburg und die weitere Region hängt aber gerade vom Projekt Trinity im Grunde die Zukunft ab. Trinity ist der Name für eine Elektrolimousine, die für das autonome Fahren des Levels 4 ausgelegt ist. Das bedeutet, dass das Fahrzeug selbst in einem komplexeren Verkehrsumfeld eigenständig navigiert. Der Fahrer kann aber noch eingreifen. Für Trinity baut VW in Warmenau eine zwei Milliarden Euro teure neue Fabrik. Schlechte Nachrichten über Sicherheitslücken kann man deshalb gar nicht gebrauchen.

Der Konzern gründete 2016 Cymotive Technologies zusammen mit hochrangigen israelischen Sicherheitsexperten. Genauer gesagt: Die drei Israelis waren zuvor hochrangige Führungskräfte des israelischen Inlandsgeheimdienstes. Israel gilt als führend auf dem Gebiet der Sicherheitstechnik. Es geht nicht nur um die Sicherheit der Fahrzeuge, sondern auch den Schutz der zunehmend vernetzten Produktion und der gleichfalls empfindlichen Logistik-Infrastruktur.

„Das Unternehmen entwirft, entwickelt und implementiert Cybersicherheitslösungen, um die größten Herausforderungen auf dem Markt für intelligente Mobilität zu lösen. Mit Teams, die in Israel, Deutschland, Schweden und den USA arbeiten, bietet Cymotive eine Plattform mit Lösungen für den gesamten Lebenszyklus sicherer Entwicklungs- bis hin zu Post-Produktionskomponenten im Ökosystem der intelligenten Mobilität an. Cymotive hat seine Reichweite erweitert und beliefert mehrere Hersteller, Smart Cities und Top-Lieferanten von Fahrzeugen, Flotten und anderen eingebetteten Lösungen", heißt es zum Firmenprofil auf der Unternehmenshomepage. Passend zum globalen Anspruch bezeichnet Cymotive seine Experten und Expertinnen als „Guardians of the Vehicle", also Wächter der Fahrzeuge.

Erstaunlich ist, dass Cymotive nun erläutert, wie eine Cyberattacke auf Volkswagen ablaufen könnten und was dagegen getan werdern kann. Im sich rasch entwickelnden Bereich der Smart Mobility seien Cyberangriffe auf Fahrzeuge bereits vorgekommen und stellten mittlerweile ein reales Problem dar. „Es ist nur eine Frage der Zeit, bis vernetzte oder autonome Fahrzeuge mit dem nächsten großen Cyberangriff konfrontiert werden", warnen die Abwehrspezialisten. Und sie verraten, wie Hacker vorgehen. In jedem Fahrzeug gibt es verschiedene Steuergeräte (Electronic Control Unit = ECU), die für unterschiedliche Vorgänge oder Funktionen im Fahrzeug verantwortlich sind. Dazu gehört beispielsweise das Infotainment-ECU, also das Multimediasystem des Fahrzeuges, oder auch das Kommunikations-ECU, welches für den ein- und ausgehenden Datenverkehr verantwortlich ist. Diese stellten beliebte Angriffsziele dar. Würden in solchen Systemen neuartige Anomalien und Exploits (Schwachstellen und Programme, die sie identifizieren) entdeckt, müsse zunächst ein Überblick über den Fahrzeugstatus hergestellt werden. Über spezielle Dashboards wird dann dokumentiert, wann das Fahrzeug aktiv war, um welches Fahrzeugmodell es sich handelt, welche anderen Anomalien entdeckt wurden sowie etwaige weitere wichtige Details. Der Rest ist Spezialistentum in Reinkultur und ein Katz-und-Maus-Spiel zwischen Kriminellen und der internen VW-Datenpolizei.

Grundsätzlich gilt laut Cymotive: Bei einem solchen Cyberangriff in der Automobilindustrie sind viele Parteien und komplexe Prozesse beteiligt. Dazu gehören Sicherheits-, Analyse- und Schwachstellenmanagementteams, die gemeinsam auf den Angriff reagieren, Schwachstellen verwalten und versuchen Risiken zu bewerten, zu minimieren und abzuschwächen. Insbesondere die Vielzahl an Anbietern und ECUs, die in einem einzigen Fahrzeug aktiv sind, stellten dabei eine große Herausforderung dar. Um von vorneherein die mögliche Angriffsfläche zu minimieren und Gefahren richtig priorisieren zu können, implementieren Unternehmen verschiedene Sicherheitstaktiken. Von zentraler Bedeutung ist dabei ein kontinuierlicher Schwachstellenmanagement-Prozess. In diesem werden fortlaufend Sicherheitslücken in den Systemen und in der eingebetteten Software identifiziert, bewertet, gemeldet und behoben.

Als Musterbeispiel beschreibt Cymotive, dass seitens des Infotainment-ECUs auffälliges Prozessverhalten gemeldet wird. Unter diese Meldung könnten viele Prozesse fallen, wie in unserem Beispiel das „Radio" und der „Display Manager", die abgestürzt waren und erneut gestartet wurden. Zusätzlich registrierte das Ethernet-ECU ausgehenden Datenverkehr, der als verboten wahrgenommen und von der Firewall blockiert wurde. Quell-IP-Adresse war die IP-Adresse des Infotainment-ECUs, die Ziel-IP-Adresse stellte sich im weiteren Verlauf der Untersuchung als bekannter Command-and-Control-Server (CNC-Server) heraus. Solche Server nutzen Cyberkriminelle, um durch Malware kompromittierte Systeme zu senden und gestohlene Daten aus dem Zielnetzwerk zu empfangen. Das Duell ist eröffnet.

Für die Experten ist eins ganz klar: „Künftig wird die Cybersecurity eines Fahrzeugs mit darüber entscheiden, ob Verbraucher ein Auto kaufen oder nicht."