# Wirtschaftsspionage gegen Volkwagen: VW-Konzern wurde jahrelang ausge…

Published: 2024-04-19 · Archived: 2026-04-05 18:50:56 UTC



VW-Modell ID.7 auf Automesse in Shanghai (2023): Hacker hatten es auf Know-how abgesehen

Foto: Ng Han Guan / picture alliance / ASSOCIATED PRESS

Bei ihren Auftritten sind die VW-Granden stets voll des Lobes für China. Bereits 2014 bei der Pekinger Automesse schwärmte der damalige Boss Martin Winterkorn von der engen Partnerschaft, die von »Kooperation, Vertrauen und Verständnis« geprägt sei. Zehn Jahre später stellt sich die Situation etwas anders dar.

Hacker, die mutmaßlich aus der Volksrepublik stammten, spionierten Volkswagen jahrelang aus, das zeigen mehr als 40 interne Dokumente, die der SPIEGEL gemeinsam mit dem ZDF einsehen konnte. Anhand der Papiere lässt sich ein groß angelegter, bislang unbekannter Cyberangriff auf Volkswagen rekonstruieren. Das offensichtliche Ziel: Know-how aus dem damals größten Autokonzern der westlichen Welt.

DER SPIEGEL 17/2024


**Vergeltung und Gegenvergeltung**

Die israelische Regierung bereitet nach dem iranischen Angriff den Gegenschlag vor. Könnte er auf das Atomprogramm der Islamischen Republik zielen? Und droht sich der Konflikt zu einem großen Krieg in der ganzen Region auszuweiten?

**Lesen Sie unsere Titelgeschichte, weitere Hintergründe und Analysen im digitalen SPIEGEL.**

Zur Ausgabe

## 19.000 erbeutete Dateien

Die Hacker nahmen das Unternehmen bereits 2010 ins Visier. 2011 und 2012 entwendeten sie Daten. 2013 verschafften sie sich Administratorrechte – und damit weitreichende Zugriffsmöglichkeiten. Gut ein halbes Jahr später, im Juni 2014, waren die Datendiebe wieder da. Neben VW griffen sie auch die Schwestermarken Audi und Bentley an.

Alle Attacken seien von denselben Tätern ausgegangen, das ist die Theorie, die laut einer internen Analyse von Volkswagen »am wahrscheinlichsten« erscheine. Bis zu 19.000 Dateien sollen die Angreifer erbeutet haben. Als »identifizierte Ziele« notierte der Konzern unter anderem »Ottomotoren-Entwicklung«, »Getriebeentwicklung« und »Doppelkupplungsgetriebe«. Auch auf Konzepte für alternative Antriebstechnologien wie Elektromobilität oder Brennstoffzellen hatten es die Unbekannten offenbar abgesehen. »Sie waren interessiert an

Getriebesteuerungs-Software, an technischen Handbüchern, wie man zum Beispiel das Direktschaltgetriebe programmiert«, berichtet einer der Experten, die mit dem Fall vertraut sind.

VW bestätigt den Vorfall, betont jedoch, dass er zehn Jahre zurückliege. Die IT-Sicherheit sei zuvor, aber auch im Nachgang massiv verstärkt worden. Darüber, wer hinter der Attacke stecke, wolle man nicht spekulieren. Die chinesische Botschaft in Berlin spricht auf Nachfrage von »Gerüchten und Unwahrheiten«, gestreut »von Menschen in den Vereinigten Staaten und anderen westlichen Ländern«. Das seien »empörende Vorwürfe, die wir entschieden zurückweisen«.

## Angriff chinesischer Staatshacker hoch wahrscheinlich

Man habe die IP-Adresse der Hacker »bis nach Peking zurückverfolgen« können, sagt ein Insider, der mit dem Vorgang vertraut ist. Die Spur führe direkt zur Volksbefreiungsarmee. Zum Schluss habe indes ein eindeutiger Beweis gefehlt. Nahezu alle Experten, mit denen SPIEGEL und ZDF gesprochen haben, darunter auch Mitarbeiter deutscher Sicherheitsbehörden, halten einen Angriff chinesischer Staatshacker für hoch wahrscheinlich.

Sowohl die im VW-Hack eingesetzte Spionagesoftware als auch die Methodik der Angreifer tragen ihre Handschrift. Sie verwendeten Programme wie PlugX oder China Chopper, die fast ausschließlich von Hackern aus der Volksrepublik verwendet wurden, sagt ein Experte.

Zunächst gelang es den Angreifern, das VW-Netzwerk am mexikanischen Standort Puebla zu infiltrieren und sich bis nach Wolfsburg vorzuarbeiten. Am 3. Juni 2014 unterlief ihnen jedoch ein entscheidendes Missgeschick. Statt sich still und heimlich im Netzwerk umzuschauen, begingen sie einen Tippfehler, der dazu führte, dass das IT-System ungewöhnlich viele Kapazitäten benötigte. Als ein VW-Techniker das System inspizierte, fielen ihm die Hacker auf.

VW-Boss Winterkorn 2007: Enge Partnerschaft, die von »Kooperation, Vertrauen und Verständnis« geprägt sei

Foto: Arne Weychardt / Wirtschaftswoche

VW stellte umgehend eine Taskforce zusammen. Monatelang beobachtete das Team die Aktivitäten der Angreifer. Am 24. April 2015, einem Freitag, schlug der Konzern zurück. Knapp zwei Dutzend Personen versammelten sich in einer Art War Room auf dem Wolfsburger Werksgelände, einige hatten sich Matratzen mitgebracht.

Für 48 Stunden wurden weite Teile des Netzwerks der VW-Gruppe heruntergefahren, mit Ausnahme von Systemen, die unbedingt laufen mussten. In der Zentrale stand ein Telefon, eine Dauer-Konferenzschaltung war eingerichtet. Jeder, der an diesem Wochenende im Einsatz war und auf Probleme stieß, egal ob in Argentinien, den Vereinigten Staaten oder in Ingolstadt, konnte sie über diese Leitung besprechen.

## »Operation am offenen Herzen«

Die Wochenendoperation begann um zehn Uhr deutscher Zeit, also 16 Uhr in China. »Wir wussten, um 16 Uhr hören die Hacker auf zu arbeiten«, berichtet einer, der mit dem Fall vertraut ist. Auch am Wochenende arbeiteten sie nicht, sie hatten – so analysierten es die IT-Sicherheitsleute in Wolfsburg – offenbar einen geregelten Bürojob

mit festen Arbeitszeiten. Deshalb schien das Wochenende ein guter Zeitpunkt, um ihre Zugänge zu kappen. Am Ende löschte das Team die Daten von mehr als 90 Servern und installierte sie neu.

Manche Fachleute sprechen im Rückblick von einer »Operation am offenen Herzen«, andere bezeichnen den Cyberangriff als seinerzeit größten weltweit. So viele Systeme habe man noch nie auf einen Schlag neu aufsetzen müssen, teilte der ebenfalls eingeschaltete Microsoft-Konzern damals laut der Unterlagen mit.

Der Vorfall führte VW schmerzlich vor Augen, was Industriespionage bedeutet. Der Konzern hat nach dem Hackerangriff die IT-Infrastruktur umgebaut. Das sei ohnehin geplant gewesen, auch vor dem Angriff, wie eine Quelle erzählt. Am Ende kostete die Hochrüstung der IT-Sicherheit einen niedrigen dreistelligen Millionenbetrag.

Der Gesamtschaden des Ideendiebstahls dürfte deutlich höher liegen. Wie die Hacker die geklauten Daten tatsächlich verwertet haben, welche Produkte daraus womöglich entstanden sind, ließ sich damals nicht ermitteln. Die groß angelegte Cyberattacke zeigt jedoch, mit welch skrupellosen Mitteln der globale Wettlauf um die Vorherrschaft in der Antriebstechnologie der Zukunft geführt wird. Und wie viel dabei für alle Seiten auf dem Spiel steht.

---