HACKERANGRIFFE

Bis zum bitteren Ende

Rund 200 VW- und Audi-Autohäuser waren von einem heimtückischen Hackerangriff betroffen. Wie man sich dagegen wappnen kann, verrät hier VAPS-Chef Wolfram Müller im Interview.

Jüngst erreichte eine neue E-Mail-Welle mit Erpressungstrojanern – auch Ransomware genannt – die Autohäuser mit teilweise katastrophalen Auswirkungen für die Betriebe. Innerhalb einer Woche erhielten ca. 200 Unternehmen diese Erpressungssoftware. Warum die kriminellen Machenschaften zunehmen und was man dagegen unternehmen kann, erklärt uns VAPS-Chef Dr. Wolfram Müller im Gespräch.

asp: *Herr Müller, warum nehmen die Viren-Angriffe auf Autohäuser stetig zu?*
W. Müller: Mit zunehmender Digitalisierung im Automobilgeschäft steigt die Online-Präsenz von Autohändlern und deren Einsatz internetfähiger Geräte immens an. Dies ist notwendig, um an neuen Geschäftsmodellen teilzunehmen, das macht sie aber gleichzeitig zunehmend angreifbarer. Außerdem hat der Handel Zugang zu großen Automobilherstellern wie Volkswagen. Dies erhöht das Risiko, Opfer eines Angriffs von Kriminellen zu werden. Diese Themen und die Konsequenzen der Digitalisierung sind ein zentraler Teil unserer Roadshows, die wir momentan VW- und Audi-Händlern anbieten.

asp: *Aber reichen denn die viel gepriesenen Virenprogramme nicht aus?*
W. Müller: Die nutzen nichts, wenn sie vom Menschen umgangen werden.

asp: *Wie das?*
W. Müller: Hierzu ein Beispiel: Ein Softwareexperte namens Drescher hatte jüngst ein Programm gegen eine Schadsoftware namens Petya entwickelt. Vermutlich als Rache für die aktive Bekämpfung und Entschlüsselung von Petya wurde Herr Drescher namentlich in die neue Angriffswelle integriert. Und zwar bekamen Personalabteilungen von Autohäusern vermeintliche, sehr professionelle Bewerbungen von Herrn Drescher zugeschickt – zum Teil tatsächlich bezogen auf aktuelle Stellenanzeigen. Leider wurde der ein oder andere Anhang von den Mitarbeitern im Autohaus sorglos geöffnet und der Weg für kriminelle Machenschaften frei. Hier hat der Mensch die Technik ausgehebelt.

asp: *Wie arbeitet eigentlich eine solche Schadsoftware?*
W. Müller: Durch das Öffnen entsprechender Makros in angehängten Excel-Tabellen wird der eigentliche Virus erst lokal als ausführbare Datei erstellt und beginnt beispielsweise lokal und im Netzwerk zugängliche Dateien zu verschlüsseln. Der User hatte somit keinen Zugang mehr auf seinen Rechner. Bei unseren VW- und Audi-Händlern umfasste der Angriff rund 200 Autohäuser.

asp: *Und bei wie vielen war der Angriff erfolgreich?*
W. Müller: Glücklicherweise konnten wir in 96 Prozent der Fälle dank unserer Software den Verschlüsselungsprozess erfolgreich abwehren. Bei den restlichen vier Prozent nahm die Schad-Software ihre Arbeit auf. In der Regel sollen die Geschädigten eine gewisse Gebühr in Bitcoins bezahlen und anschließend eine Entschlüsselungssoftware bekommen. Was aber in den meisten Fällen nicht passiert, da es sich dabei um reinen Betrug handelt. Mein Tipp: Niemals auf Zahlungsforderungen jeglicher Art eingehen.

asp: *Wie merke ich, dass mein Rechner infiziert wurde?*
W. Müller: Selbst wenn Anhänge angeklickt und Makros aktiviert werden, besteht noch Hoffnung. Ein Indiz für einen Angriff ist zum Beispiel, wenn der Rechner eigenständig herunterfährt und wieder einen Neustart anstrebt, mit dem Hinweis, dass ein Reparaturprozess startet. In einem solchen Fall heißt es: Rechner sofort vom Netz nehmen und physisch isolieren, bevor er erneut vollständig rebooten kann.

Foto: VAPS

VAPS-Chef Wolfram Müller: „Man braucht eine funktionierende Datensicherung, die physisch vom System getrennt ist. Und wir empfehlen Autohäusern, eine Segmentierung der gesamten IT-Struktur vorzunehmen."

Der sicherste Fall ist natürlich, wenn ein aktuelles Virenschutzprogramm anspricht und das Virus selbstständig entfernt oder zumindest einen Hinweis auf einen möglichen Befall gibt.

asp: *Wie kann man sich gegen solche Angriffe wehren?*
W. Müller: Beispielsweise mittels aktueller Virenschutzprogramme. Diese registrieren sehr schnell, dass etwas im Prozessverlauf nicht mit rechten Dingen zugeht, und sprechen eine Warnung aus. Eine wichtige Regel lautet: niemals Makros in fremden Dokumenten aktivieren!

asp: *Und wenn das doch passiert sein sollte?*
W. Müller: Dann entsteht unter Umständen ein immenser Schaden für das Autohaus. Sollte keine regelmäßige Datensicherung erfolgen, dann können sämtliche Informationen für immer verloren sein. Das kann unter Umständen für ein Autohaus den Ruin bedeuten.

asp: *Wie sieht eine permanente Datensicherung konkret aus?*

W. Müller: Man braucht eine funktionierende Datensicherung, die physisch vom System getrennt ist. Diese sollte täglich erfolgen und regelmäßig geprüft werden, ob ein Restore mit dem Backup tatsächlich funktioniert. Erfolgt mit diesem Status ein erfolgreicher Hackerangriff, so ist in der Regel nach ein bis drei Tagen ein normaler Betrieb wieder möglich. Wenn keine Datensicherung erfolgt ist, heißt es im schlimmsten Fall: Pech gehabt. Die Daten sind für immer verloren. Das System muss von Grund auf neu aufgebaut werden, was nicht nur ein Autohaus, sondern auch die komplett vernetzte Gruppe treffen kann. Man kann nicht mehr arbeiten. Im Falle eines vorhandenen Dealer-Management-Systems in einer Cloud könnte eventuell „nur" das Outlook unbrauchbar sein. Hier fängt man aber ebenfalls bei null an.

asp: *Gibt es noch andere Methoden, Schäden einzudämmen?*
W. Müller: Wir empfehlen Autohäusern, eine Segmentierung ihrer gesamten IT-Struktur vorzunehmen. Das bedeutet praktisch: Ein Mitarbeiter der Personalabteilung hat keine Zugriffsrechte auf vertriebliche Laufwerke. Ein Virus im Segment Personalabteilung legt in einem Schadensfall nur diesen Bereich lahm, die anderen bleiben davon unberührt. Der Schaden wäre überschaubar und eingegrenzt. Ein aktueller Antiviren-Client sollte auf jedem Endgerät sowieso Pflicht sein. Die Absicherung des Zugangs zum Internet durch eine moderne Firewall-Lösung sollte ein weiteres Ziel sein.

KURZFASSUNG

In 96 Prozent der von Hackern attackierten Autohäuser konnte der Angriff erfolgreich abgewehrt werden. Wolfram Müller, Geschäftsführer der VAPS GmbH (Volkswagen und Audi Partnerverband), erläutert hier, woran man Hackerangriffe erkennt und wie man sich in diesem Fall verhalten sollte.

asp: *Wie sieht Ihre Prognose aus?*
W. Müller: Fakt ist, dass massive Angriffe aus dem Internet extrem zunehmen werden. Die Gefahrenlage ist hoch und wächst kontinuierlich, da immer mehr sensible Datenmengen anfallen. Pauschal kann man sagen, dass man mittlerweile immer mit kriminellen Machenschaften rechnen muss. Die Angriffswellen werden weitergehen.

asp: *Was raten Sie Autohäusern?*
W. Müller: Die Händler sollten ein Bewusstsein für die steigenden Gefahren entwickeln und ihre Mitarbeiter in allen Bereichen mit einbeziehen – auch den Servicebereich, wo teilweise bereits Tablets mit Internetzugang im Einsatz sind. Das Thema Netzwerksicherheit betrifft den kompletten Betrieb und jeden Mitarbeiter. Der Hersteller Volkswagen hat mit dem BK2018 eine umfassende Handlungsempfehlung bereitgestellt, welche die IT-Struktur der Betriebe auf die kommenden Anforderungen vorbereitet und umgesetzt werden sollte. Eine umfassende Beratung von Spezialisten ist absolut empfehlenswert.

Interview: Thomas Maier