Bodyguards der Straße

Längst steht auch das Auto unter Beschuss aus dem Internet. Im schlimmsten Fall ist das Leben der Passagiere in Gefahr. Höchste Zeit für eine Cyberleibwache, die bei Hackerangriffen in Echtzeit eingreift.

TEXT —— Yvonne Schmitz

Kevin Costner weiß, wie man Menschen beschützt: Im Film „Bodyguard“ entreißt der Schauspieler die Popsängerin Rachel – gespielt von Whitney Houston – einem tobenden Fanmob und flieht mit ihr in einer Limousine, deren Fahrer er zuvor ein Extremfahrtraining verpasst hat.

Der Blockbuster ist von 1992 – heute würde die Szene wohl anders aussehen. Um sich gegen Angriffe zu schützen, reichen ein geschickter Chauffeur und griffige Reifen allein nicht mehr aus. Digitale Abwehrkräfte gehören heute ebenfalls dazu. Schließlich sind mittlerweile – je nachdem, welche Studie man heranzieht – zehn bis 30 Prozent aller Fahrzeuge mit dem Internet vernetzt, Tendenz steigend. Das bedeutet nicht nur mehr Komfort durch digitale Dienste wie einen rollenden Hotspot, sondern lockt auch Hacker auf den Plan. Ohne wasserdichte Schutzmaßnahmen könnten Cyberkriminelle per Internet von überall auf der Welt auf ein Fahrzeug zugreifen – ein Feind, vor dem selbst Kevin Costner nicht davonfahren könnte.

Dass Autos gegen Sicherheitslücken nicht gefeit sind, zeigt das jüngste Beispiel: Im September 2018 etwa veröffentlichten belgische Experten eine Schwachstelle im Funkschlüssel von Teslas Model S, dank der sie den Schlüssel in Sekundenschnelle klonen und das zugehörige Auto öffnen und starten konnten. Erfreulich für Autodiebe, fatal für Autohalter.

SICHERHEIT VON ANFANG AN

Die Automobilbranche hat die Gefahr erkannt und rüstet cybertechnisch auf. Die Kanzlei Foley & Lardner hat Automobil- und Technologiemanager aus den USA und Asien zur Entwicklung vernetzter und autonomer Fahrzeuge befragt: Fast zwei Drittel gaben an, Cyberattacken zu bedenken. Zudem haben die 15 Autobauer des Europäischen Automobilverbunds ACEA ihre Bereitschaft signalisiert, sich über neue Cybersecuritygefahren mit öffentlichen Behörden, Industrieakteuren und Dritten auszutauschen. Aber genügt das? „Egal, wie sorgfältig Fahrzeuge in Sachen IT-Sicherheit entwickelt werden: Es kann immer eine Sicherheitslücke bleiben – oder mit der Zeit erst entstehen“, warnt Christian Olt, Senior Security Manager im Bereich Automotive & Manufacturing bei T-Systems. Deswegen braucht das Auto einen digitalen Bodyguard, der Cyberangriffe während seiner gesamten Nutzungsdauer erkennt und im Notfall sofort abwehrt: ein Automotive Security Operation Center (SOC).

SCHARFER AUFPASSER AN BORD

In einem solchen Automotive SOC fließen alle sicherheitsrelevanten Daten aus dem Fahrzeug und seiner Umgebung zusammen. Eine wichtige Datenquelle ist dabei ein Angriffsdetektionssystem im Auto (Intrusion Detection System, IDS). Die Automobilbranche arbeitet bereits intensiv an der Integration solcher Systeme. Doch auch Auffälligkeiten im Mobilfunknetz und Hersteller-Backend sind relevant. Ein Beispiel: Unerwartete Nachrichten im Bordnetz müssen nicht unbedingt von einem Eindringling stammen. Liefen aber kurz davor unübliche Prozesse in den Datenbanken des Fahrzeugherstellers, steigt die Wahrscheinlichkeit eines Hackerangriffs.

Zusätzlich helfen externe Informationen, Cyberattacken zu identifizieren. Die „Threat Intelligence“ nutzt zum Beispiel vorhandene Listen bösartiger IP-Adressen, Hinweise von wohlgesinnten Sicherheitsexperten und anderen SOCs oder künftig auch spezielle Honeypots: Autosimulationen, die Hacker gezielt anlocken und auf diese Weise neue Angriffsmuster aufdecken.

SCHNELLE GEGENWEHR DANK SIEM-SYSTEM

Ein spezielles System – das Security Information and Event Management (SIEM) System – analysiert und korreliert alle Daten. Findet das System Hinweise für eine Cyberattacke, alarmiert es über ein Dashboard die Securityanalysten im Automotive SOC. Diese nehmen sich dann des Vorfalls an. Sie prüfen die Meldungen auf Fehlalarme und führen eigene Recherchen durch. Die ganz harten Fälle landen bei den digitalen Detektiven der Sicherheitszentrale: den IT-Forensikern. Sie durchleuchten kompromittierte Systeme im Detail und versuchen, das Vorgehen des Täters zu rekonstruieren. Falls nötig, sichern sie dafür Daten aus betroffenen Fahrzeugen direkt vor Ort.

Doch wie schlagen die Spezialisten des Automotive SOC im Ernstfall Angreifer in die Flucht? Dieses Prozedere ist genau

Der Vormarsch vernetzter Fahrzeuge:

Ob ein Auto einen Internetzugang hat, ist künftig keine Frage der individuellen Ausstattung mehr. Zumindest nicht in der EU: Seit dem 31. März 2018 müssen alle neuen Fahrzeugmodelle mit dem automatischen Notrufsystem eCall ausgestattet sein, um eine Typgenehmigung zu bekommen – also die staatliche Erlaubnis für ihre Produktion. Das System beinhaltet eine SIM-Karte und damit auch den Draht ins Internet. eCall setzt bei einem Unfall automatisch einen Notruf ab. So will die EU-Kommission 2.500 Menschenleben pro Jahr retten.

Foto: iStockphoto

3.300

Datenquellen liefern Daten für das Security Operation Center der Deutschen Telekom.

12 Mio. Angriffe

registrieren die Honeypot-Sensoren im Telekom-Netz täglich.

1,5 Mrd.

sicherheitsrelevante Events analysiert das Security Operation Center der Telekom pro Tag.

festgelegt: Ein Incident Response Plan definiert, welche Schritte die Securityanalysten bei welchem Alarm durchzuführen haben. „Schadsoftware zum Beispiel kann sich in Sekunden bis Minuten in einem Netzwerk ausbreiten", erklärt Olt. „Da bleibt keine Zeit für Diskussionen. Je schneller die Abwehrreaktion, desto weniger Schaden entsteht." Im Idealfall legt der Automobilhersteller daher auch fest, wie schnell sich ein Analyst eines Alarms annehmen muss.

Besonders bei sehr kritischen Vorfällen oder wenn die Gegenmaßnahme nicht unbemerkt bleiben wird, braucht das Automotive-SOC-Team klare, abgestimmte Handlungsanweisungen oder muss Entscheider einbinden. Also etwa dann, wenn eine kompromittierte Auto-SIM-Karte immer wieder teure Hotlines anruft und das SOC-Team das Mobilfunkmodul deswegen deaktivieren möchte – damit aber auch Dienste wie die Echtzeitnavigation abschalten würde.

SICHERGEHEN BEIM DATENSCHUTZ

Ein wichtiger Aspekt bei der Arbeit mit Daten für ein Automotive SOC ist der Datenschutz. Der deutsche Verband der Automobilindustrie (VDA) und die Datenschutzbeauftragten von Bund und Ländern in Deutschland gehen beispielsweise davon aus, dass alle Daten personenbezogen – und damit datenschutzrelevant – sind, die mit dem Kennzeichen oder der Identifikationsnummer des Fahrzeugs (VIN) in Verbindung stehen. Das gilt etwa für GPS-Daten oder die Fahrzeuggeschwindigkeit. Problematisch hierbei: Auch ohne direkten Personenbezug können manche Daten auf einen bestimmten Passagier hindeuten, zum Beispiel die Motordrehzahl, welche vom Fahrstil des jeweiligen Autofahrers abhängt. „Wollen Automobilhersteller auf der sicheren Seite sein", sagt Olt, „empfehlen wir, alle Daten für ein Automotive SOC als personenbezogen zu erklären."

Das SOC selbst muss für seine Analyse aber gar nicht wissen, zu welchem konkreten Fahrzeug oder welcher Person die Daten gehören. Deswegen sollten Automobilhersteller diese Informationen noch vor der Übertragung an die Cyberabwehrzentrale anonymisieren oder pseudonymisieren. Letzteres bietet sich immer dann an, wenn der Fahrzeughersteller den Personenbezug später wiederherstellen möchte – um beispielsweise den Fahrzeughalter zu kontaktieren. Bei einer Anonymisierung ist das nicht möglich.

EXPERTEN MIT DOPPEL-KNOW-HOW

Security Operation Center sind an sich nichts Neues. Zum Schutz der Unternehmens-IT gibt es sie in vielen Branchen – auch in der Automobilindustrie. Die klassischen IT-SOCs kennen sich allerdings weder mit Autotechnik noch mit fahrzeugspezifischen Bedrohungen aus. Deswegen erfordert die Cyberabwehr für vernetzte Autos eine eigene spezialisierte Sicherheitszentrale, die Kompetenzen aus beiden Fachbereichen verbindet: IT-Sicherheit und Fahrzeug-IT. Ein heißer Draht zwischen beiden SOCs ist jedoch empfehlenswert, denn ein Angriff in der Arbeitsplatzdomäne könnte sich auch auf die Fahrzeugseite ausbreiten.

Seit Herbst 2017 betreibt die Deutsche Telekom eines der größten und modernsten Security Operation Center Europas. 200 Experten überwachen hier und an den angeschlossenen weltweiten Standorten zu jeder Tageszeit die Systeme der Telekom und ihrer Kunden. Sie erkennen Angriffe quasi in Echtzeit, wehren sie ab und analysieren das Vorgehen der Cyberkriminellen, um die eigene Sicherheitstechnik zu optimieren. Wichtige Informationen liefern dabei die 2.200 weltweiten Honeypots im Netz der Telekom.

Auch das für ein Automotive SOC notwendige Automobil-Know-how ist fest in der DNA des Konzerns verankert: Die Telekom-Tochter T-Systems unterstützt viele große Fahrzeughersteller, -zulieferer und Autohäuser zum Beispiel dabei, vernetzte und autonome Autos zu entwickeln. „Mit unserer Erfahrung in den Bereichen Security und Automotive können wir Automobilherstellern helfen, eine spezialisierte Cyberabwehr für das vernetzte Fahrzeug aufzubauen", betont Olt. „Je nach Bedarf übernehmen wir im Betrieb auch ausgewählte Rollen wie beispielsweise die standardisierte Erstanalyse von Sicherheitsalarmen."

In einer Neuverfilmung von „Bodyguard" könnte Kevin Costner dann den Angriff eines Hackers, der aus der Ferne die Kontrolle über Whitney Houstons Limousine übernommen hat, mit einem Griff zum Telefon abwehren: indem er seine Cyberkollegen einfach bittet, die Mobilfunkverbindung des Autos zu unterbrechen.

Christian.Olt@telekom.de