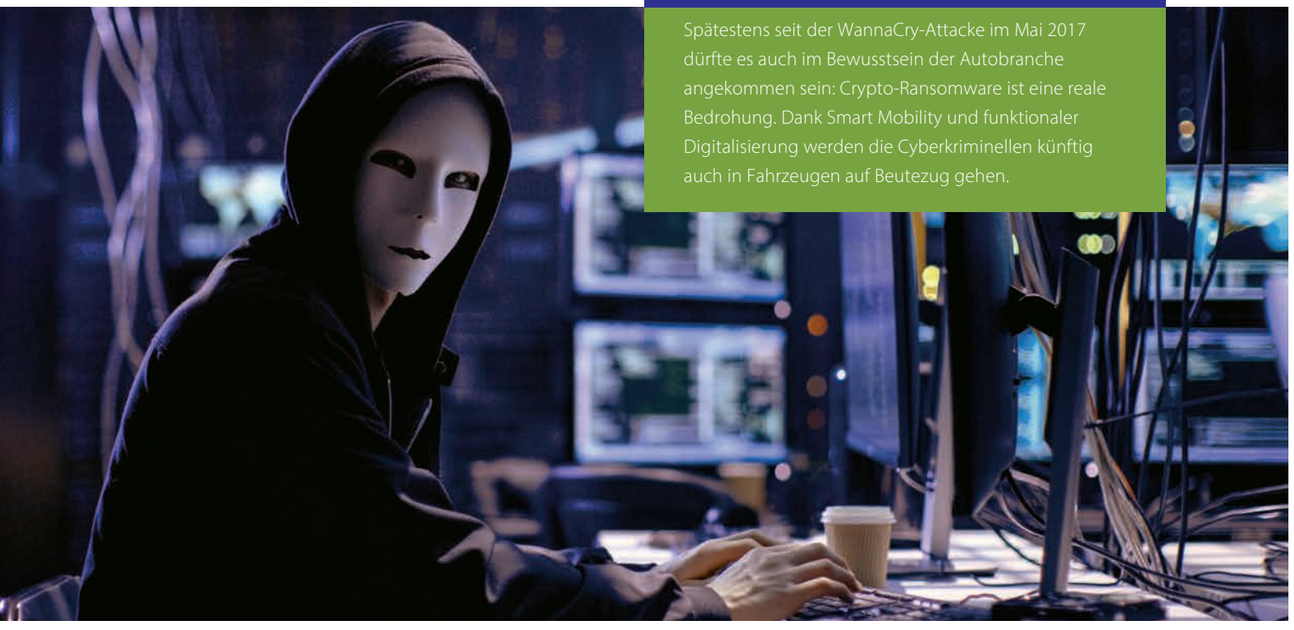
Lösegeldforderung aus dem Armaturenbrett

WannaDrive? Gegen Automotive- Ransomware hilft ganzheitliche IT-Security



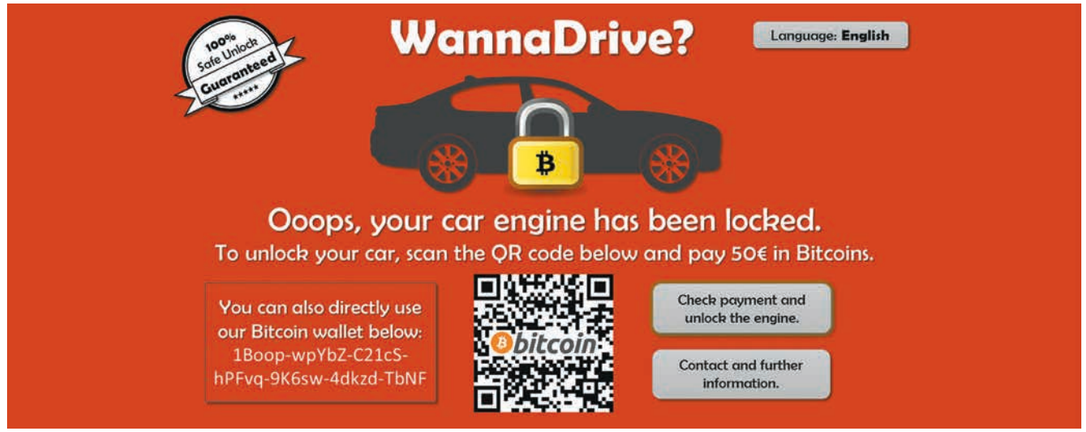
Spätestens seit der WannaCry-Attacke im Mai 2017 dürfte es auch im Bewusstsein der Autobranche angekommen sein: Crypto-Ransomware ist eine reale Bedrohung. Dank Smart Mobility und funktionaler Digitalisierung werden die Cyberkriminellen künftig auch in Fahrzeugen auf Beutezug gehen.

Ins Visier der Online-Erpresser werden dabei vor allem kommerzielle Fahrzeuge und Fahrzeugflotten geraten: Lastwagen etwa, die engen Lieferplänen folgen oder verderbliche Güter transportieren, Busunternehmen, Mietwagen- und Carsharing-Flotten, teure Baumaschinen und Spezialfahrzeuge etc. Gelingt es den Online-Erpressern, diese per Ransomware in digitale Geiselhaft zu nehmen, dann haben sie gute Erlöschancen.

Ransomware-Attacken mit geringem Aufwand realisierbar

Obwohl bis dato keine erfolgreichen Ransomware-Attacken auf Fahrzeuge bekannt sind, lässt sich aus der angewandten Praxis in anderen Bereichen sehr wohl ein typisches Angriffsszenario ableiten. Cyberkriminelle greifen hier zumeist auf bereits existierende Ready-to-use-Ransomware-Kits oder Ransomware-as-a-Service-Angebote zurück, Bot-Master und Bitcoin-Bezahlsystem inklusive. Bislang zielen solche Ransomware-Kits vor allem auf klassische Desktops und Server-IT. Aber mit steigender Zahl angreifbarer Fahrzeuge und erpressbarer Flottenbetreiber im digitalen Netz werden unweigerlich auch Ransomware-Varianten für Automotive Linux oder AUTOSAR auftauchen.

Die möglichen Einfallstore für Ransom-Malware indes sind heute schon zahlreich – Webseitenaufrufe über das Infotainment-System, im Fahrzeug empfangene Nachrichten (z. B. per E-Mail, SMS, Messengerdienst oder Digitalradio), ans Fahrzeug angeschlossene Smartphones oder Navigationsgeräte, FOTA-Updates, Ferndiagnosen oder Cloud-Services des Autoherstellers.



Hat die Ransom-Malware erst einmal das System gekapert, lässt sich das Fahrzeug nur schwer aus der digitalen Geiselhaft befreien

Sicherheitsingenieure von ESCRYPT haben eine solche Ransomware-Attacke bereits „erfolgreich" am Modell simuliert. Ein Raspberry Pi mit Linux OS und Touchscreen als automobiles Infotainment-System wurde dabei mit einem echten Tachometer-Steuergerät mit Originalhersteller-Firmware über eine Gateway-ECU und ein proprietäres Busnetzwerk verbunden – ähnlich wie es in einem normalen Fahrzeug auch der Fall wäre. Der Raspberry als Host-ECU wurde mit einer Python-basierten Ransomware über die USB-Schnittstelle „infiziert". Wie beabsichtigt, blockierte der Ransomware-Client daraufhin den Tachometer und stellte dessen Geschwindigkeitsanzeige permanent auf Höchstgeschwindigkeit. Zugleich erschien auf dem Touchscreen des „Infotainment-Systems" die Lösegeldforderung mit Zahlungsanweisung auf ein anonymes Bitcoin-Konto (Bild oben). Das Fazit: Ransomware-Attacken auf Fahrzeuge sind eine echte, leicht zu realisierende Bedrohung – sofern das Niveau der IT-Security nicht der zunehmenden Vernetzung der Autos angepasst wird.

Ganzheitlicher Security-Ansatz beugt vor

Heutige Fahrzeuge bieten zwar bereits zahlreiche Angriffspunkte, halten aber oft kein Backup für wichtige Daten und Funktionalitäten vor. Sie erhalten außerdem keine regelmäßigen Security-Updates, verfügen meist nur über einfache (Gateway-)Firewalls und selten über Systeme zur automatischen Angriffserkennung und -abwehr. Hier nachzubessern ist meist schwierig und kostenintensiv. Am wirksamsten lässt sich Fahrzeug-IT gegen Ransomware und andere Cyberattacken schützen, indem die Hersteller von vornherein, bei der Entwicklung der Fahrzeugplattform umfassend wirksame IT-Sicherheit verankern. Ein solcher ganzheitlicher Ansatz muss das gesamte Fahrzeugsystem einschließlich seiner IT-Infrastruktur, den gesamten Fahrzeuglebenszyklus bis hin zur Stilllegung sowie die gesamte Organisation, inklusive festgelegter Security-Prozesse und Security-Governance, einbeziehen.

Der ganzheitliche Schutz des Fahrzeugs verlangt demnach nach einer Reihe ineinandergreifender Security-Maßnahmen: Im Fahrzeug selbst helfen eingebettete Security-Komponenten, Hacker-Angriffe und Schadsoftware mit bekannten Signaturen abzuwehren. Auch werden über ein Intrusion Detection and Prevention System (IDPS) kritische Anomalien in der Bordnetzkommunikation wie etwaige Ransomware-Angriffe erkannt und ausgeschaltet – entweder direkt im Fahrzeug oder über ein angebundenes Security Operations Center (SOC) im Backend, das bei einem neu erkannten Angriffsmuster entsprechend wirksame Security-Updates für die gesamte Fahrzeugflotte verteilen kann. Und sollte eine Ransomware-Attacke doch einmal Erfolg haben, braucht es eine schnelle, wirkungsvolle Reaktion, beispielsweise mithilfe zuvor festgelegter „Incident Response Procedures", die Gegenmaßnahmen vorgeben – notfalls bis hin zur Lösegeldzahlung.

Die potentielle Bedrohung durch Ransomware im Auto führt eines deutlich vor Augen: Ganzheitlich wirksame Automotive Security ist kein lästiger Kosten-, sondern ein entscheidender Erfolgsfaktor. Sie hilft Flottenbetreibern und Autoherstellern, sich gegen Online-Erpressung, Rückrufaktionen und Schadensersatzforderungen zu wappnen. ■

Autor

Dr.-Ing. Marko Wolf ist Head of Consulting & Engineering bei **ESCRYPT**.