Editorial ::

Game Over?

Liebe Leserinnen, liebe Leser,

Ende März veranstaltete der MAS e. V. in München seine 89. Tagung. Unter den vielen interessanten Beiträgen befasste sich Dr. Nils Weiß von der dissecto GmbH mit dem Thema "Automotive Security". Weiß verbindet eine langjährige Zusammenarbeit mit der Versicherungswirtschaft und mit dem AZT in Ismaning – insbesondere, wenn es um gestohlene Fahrzeuge geht, ist seine Expertise gefragt. Dafür braucht es Erfahrung, tiefe Einblicke in Sicherheitssysteme und eine umfassende Beobachtung der Entwicklungen am Markt.
Was Weiß beim MAS zu berichten hatte, lässt Verbraucher, Tuner, Werkstätten, Sachverständige und alle anderen, die Daten und Informationen aus modernen Fahrzeugen gewinnen wollen, wenig zuversichtlich in die Zukunft blicken. Denn alle Fahrzeughersteller setzen zunehmend auf Abschottung, und Zugriffsversuche von außen werden von der Fahrzeugelektronik als Angriff und Bedrohung gewertet. Weiß: "Aufgrund der proprietären Systeme und Komponenten in der Automobilindustrie ist ein hoher Aufwand für Reverse Engineering notwendig, um an realen Systemen forschen zu können."
Spezialisierte und weltweit agierende Hacker-Firmen investieren bis zu zwei Jahre und drei Personen Manpower in den Hack moderner Fahrzeuge, um anschließend den Fahrzeughersteller zu erpressen oder zur Kooperation zu bewegen. Schwachstellen in der Fahrzeugelektronik werden weitgehend geheim gehalten oder inzwischen bei vielen Marken kurzfristig durch Over-The-Air-Updates (OTA) beseitigt.
Mehrstufige Sicherheitskonzepte, zentrale Hochleistungsrechner, steigende Komplexität in vernetzten und automatisierten Fahrzeugen umfassen Security-Maßnahmen auf allen Ebenen der Fahrzeugarchitektur und -kommunikation – vom Mikrocontroller bis zur Infrastruktur. Angriffe werden automatisch erkannt, der Austausch von Teilen wird erschwert, die Diagnose liegt vollständig in der Hand der OEMs, Daten werden hochsicher im Fahrzeug gespeichert. Werkstatttester benötigen eine Authentifizierung, die ohne Internetverbindung quasi unmöglich ist, und die volle Kontrolle liegt beim Fahrzeughersteller.
Der Verschlüsselung zur Gewährleistung der Cybersicherheit stehen die Anforderungen des freien Zugangs für alle Marktbeteiligten gegenüber und die aufgebauten Hürden werden immer höher. Kein Hersteller wird mehr seine Sicherheit schwächen, um eine Offline-Diagnose möglich zu machen. Wer sich nicht mehr authentifiziert, dem bleibt bald sogar die Fehlerauslese verwehrt.

Mit besten Grüßen, Ihr

Thomas Seidenstücker, Chefredakteur VKU

Inhalt ::

Foto: Adobe Stock 16229074