Von A bis Z durchgetestet

Security-Tests für den gesamten Fahrzeuglebenszyklus

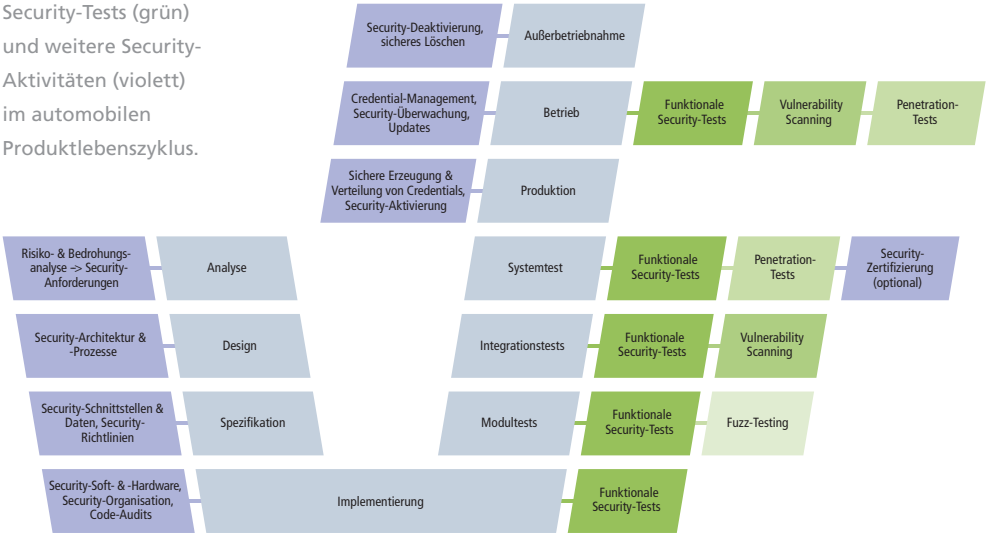
AUTOREN

Dr. Markus Kögel ist Expert Security Consultant bei der **ESCRYPT GmbH**.

Dr.-Ing. Marko Wolf ist Head of Consulting und Engineering bei der **ESCRYPT GmbH**.

ESCRYPT ist eine hundertprozentige Tochtergesellschaft von ETAS und bietet Sicherheitslösungen im Bereich Embedded Security an.

Wirkungsvolle Informationssicherheit erfordert Security-Tests während des gesamten Fahrzeuglebenszyklus. Denn im Gegensatz zu klassischen Tests zur Fahrsicherheit, bei denen sich die meist durch physikalische Gesetzmäßigkeiten bestimmten Randbedingungen später nicht mehr ändern, unterliegen die Annahmen und Randbedingungen der Security-Tests dem ewigen Wettstreit zwischen Angreifer und Verteidiger. Deshalb sind auch nach Produktionsstart bis zur Außerbetriebnahme des Fahrzeugs regelmäßige Security-Tests notwendig, um auch neu entwickelte Cyberangriffe und bisher unentdeckte Sicherheitslücken zu prüfen und notfalls noch effektiv darauf reagieren zu können.



Security-Tests (grün) und weitere Security-Aktivitäten (violett) im automobilen Produktlebenszyklus.

Automotive-Security-Testmethoden für jede Phase

Die Security-Tests im Automobilbereich (Automotive Security Testing) unterscheiden im Wesentlichen vier verschiedene Testmethoden, die im erweiterten V-Modell der aufsteigenden Flanke verortet sind (siehe Grafik), konkret: funktionale Security-Tests (Functional Security Testing), automatisierte Schwachstellensuche (Vulnerability Scanning), Fuzz-Testing (Fuzzing) und sogenannte Penetration-Tests. In all diesen Bereichen bietet ESCRYPT umfangreiche Beratung und Dienstleistung an.

Funktionale Security-Tests werden eingesetzt, um zu prüfen, ob die Spezifikation der verwendeten Security-Mechanismen korrekt und vollständig umgesetzt wurde. Das Vorgehen ist sehr ähnlich zu klassischen funktionalen Tests, der Fokus wird hier allerdings auf die Security-Funktionalität gelegt. Dabei wird sowohl die Implementierung – beispielsweise von Verschlüsselungs- oder Authentifizierungsalgorithmen – auf Fehlerfreiheit getestet als auch die Performance und der Ressourcenverbrauch der Implementierung betrachtet, um zum Beispiel mögliche Konflikte mit Laufzeitanforderungen oder Speicherbedarfen zu identifizieren.

Fuzzing-Tests werden zusätzlich zu den funktionalen Security-Tests angewendet, um systematisch durch verschiedene unerwartete, ungültige oder unplausible Nachrichten ein instabiles oder gar fehlerhaftes Verhalten des Systems aufzudecken.

Vulnerability Scanning wiederum konzentriert sich auf die umfängliche Prüfung bereits bekannter Einfallstore, Sicherheitslücken und Verwundbarkeiten für Cyberangriffe. Für diese Security-Tests wird meist eine stetig aktualisierte Datenbank mit allen zu dem Zeitpunkt bekannten Schwachstellen für das Testobjekt verwendet.

Penetration-Tests untersuchen in der Regel erst die Release-Kandidaten von neuen Automotive-IT-Systemen. Diese erweiterten Security-Tests folgen dem Prinzip, dass ein IT-System nur dann ausreichend getestet ist, wenn es auch mit dem Wissen, Können und den Werkzeugen eines realistischen Angreifers umfangreich untersucht wurde.

ETAS und ESCRYPT bieten hier neben Beratung und Dienstleistung verschiedene Testsysteme an (siehe S. 12). Insbesondere ESCRYPT führt seit über einem Jahrzehnt Security-Tests für Automotive-Security-Anwendungen durch und ist Partner vieler OEMs und Zulieferer. Das ETAS-Tochterunternehmen verfügt über ein hochmodernes Testing-Labor und ist für diverse Angriffsmethoden bestens gerüstet – ganz gleich ob PEN-Testing von Hardware, Software oder Automotive-Netzwerken.