Engineering Partner

Absicherung im Umfeld Cybersecurity

Von Nicolae Foica, Teamleiter E/E Gesamtsystem Diagnoseentwicklung & -test im Fachgebiet E/E Systementwicklung bei ServiceXpert, München

Die Zahl der Cyberangriffe auf Unternehmen lag im Jahr 2021 um 50 % über dem Vorjahresniveau. Prominente Fälle, bei denen zum Teil wochenlang Produktionsstätten und unternehmerisches Handeln lahmgelegt waren, konnte man der Presse entnehmen. Deshalb haben Investitionen in Cybersecurity-Dienste und Informationssicherheit heute höchste Priorität für die Widerstandsfähigkeit und Gesundheit eines Unternehmens.

Im Zeitalter der digitalen Revolution ist die Interkonnektivität enorm gestiegen. Die verbesserte Verfügbarkeit und Online-Zugänglichkeit von Systemen steigert die Möglichkeiten von Cyberangriffen und -bedrohungen. Diese bilden eine reale Gefahr von unerwarteten Schäden und finanziellen Verlusten von Unternehmen. Dabei ist auch die Entwicklung von Fahrzeugen betroffen. Mit den neuen UNECE Regulierung R155 und R156 werden die OEMs verpflichtet, Cybersecurity Anforderungen bei der Produktentwicklung verbindlich zu berücksichtigen.

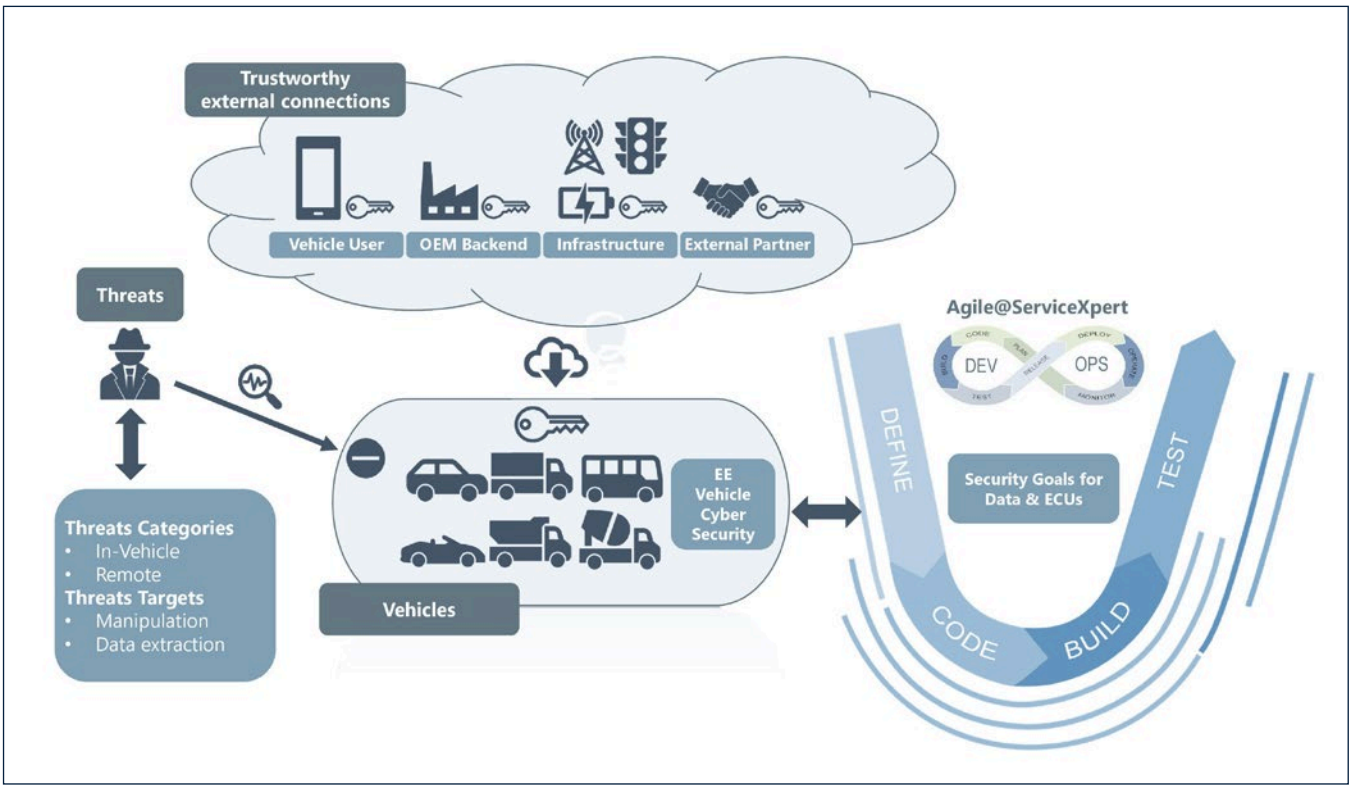
Die ServiceXpert bietet im Rahmen von Absicherungsprojekten alle relevanten Pakete für Cybersecurity-Tests von Automotive ECUs an. Die Projekte starten mit einer Sicherheitsrisikobewertung, um gefährdete Bereiche und das Ausmaß der Risiken zu bestimmen. Dies bildet die Grundlage der Planung, des Entwurfs und der Priorisierung von Sicherheitstests. Erfahrungsgemäß sollten Risikobewertungen regelmäßig durchgeführt werden, da sie nur eine Momentaufnahme zu einem bestimmten Zeitpunkt darstellen. Sicherheitsrisiken ändern sich ständig, da täglich auch neue Bedrohungen auftauchen.

In der Konzeptphase eines Cybersecurity Testprojektes werden Objekte, Cybersecurity Ziele und letztendlich das Cybersecurity Konzept selbst festgelegt. Innerhalb von TARA (Threat Analysis and Risk Assessment) werden Bedrohungen und Risiken identifiziert und Anforderungen (an die ECUs) abgeleitet.

Gemäß UNECE R155 sind Automotive OEMs verpflichtet, den Nachweis für die Umsetzung und die Absicherung von Cybersecurity Anteilen zu führen. Dazu werden Verifikationsaktivitäten durchgeführt, um zu bestätigen, dass die Implementierung des Entwurfs und die Integration der Komponenten mit den verfeinerten Anforderungen und dem Entwurf übereinstimmen.

Die Entwurfsimplementierung und die Integration des Steuergeräts werden mit den Methoden und/oder Kriterien verifiziert, die in den CAL-Leistungsmethoden (Cybersecurity Assurance Level) festgelegt sind.

Wird eine Schwachstelle identifiziert, wird ein Schwachstellenmanagement durchgeführt. Auf der Grundlage des Schwachstellenmanagements wird eine Angriffspfadanalyse und eine Bewertung der Umsetzbarkeit von Angriffen durchgeführt.



Grafik: © ServiceXpert

Basierend auf dem Analyseergebnis wird eine Teststrategie in Abstimmung mit dem Kunden entwickelt, aus der das Testkonzept abgeleitet wird. Nach Generierung von Testspezifikationen und Test Cases unter Beachtung der Traceability wird die Testdurchführung auch im Hinblick auf eine mögliche Testautomatisierung geplant und umgesetzt.

Das Testkonzept orientiert sich an den geforderten Projektschwerpunkten. Ein Projektbeispiel könnte folgendermaßen aussehen:

Test Case Entwicklung für

- Certificate Handling nach kundenspezifischen Anforderungen
- sichere Diagnose mit Verwendung von Service Authenticate 0x29
- Prüfung der Daten auf Integrität (IVD – IntegrityValidationData)
- Protokoll für die Verwaltung von Aktualisierungen von Zertifikaten und anderen Arten sensibler Daten
- Schließung der Debugschnittstelle (nach Serieneinsatz gesperrt)
- sicheres Softwareupdate zur Minderung der Risiken für den unbefugten Zugriff auf Software in ECUs

Die Umsetzung der Cybersecurity Umfänge erfolgt über die Methode „test driven development“, d. h., dass die Validierung und Absicherung einer Automotive ECU in mehreren Testrunden erfolgt.

Das Vorgehen der ServiceXpert Ingenieure orientiert sich im Allgemeinen an folgender Abfolge:

Generische und detaillierte Test Case Definition, Erweiterung mit kundenspezifischen Test Cases, Review der Testumfänge mit dem Kunden, Umsetzung von Testautomatisierung und zu guter Letzt Testdurchführung, Ergebnisanalyse und Reporting zum Kunden.

ServiceXpert setzt auf ein eigenentwickeltes Testframework unter Verwendung von in der Automotive-Industrie etablierten Tools.

Da in diesem Zusammenhang Systeme neuester Architektur und hoher Leistungsfähigkeit entwickelt werden, erfolgen die Validierungsaufgaben parallel in enger Abstimmung mit der System- und Softwareentwicklung. Es ist eine Scrum-angelehnte Vorgehensweise im Validierungsprozess erforderlich, die sich stark an die agilen Entwicklungsprozesse anlehnt. Diese Anforderungen ergeben sich daraus, dass auf kurzfristige Änderungen in der System- und Softwareentwicklung, auch in der Validierung, reagiert werden muss.

Vor dem Hintergrund neuer Normen und Standards unterstützt ServiceXpert auch im Bereich der Prozessanpassung und -verbesserung.

Neben der Bereitstellung modernster Softwareentwicklung für Geschäftspartner weltweit verfügt die ServiceXpert über ein starkes Team von Cybersecurity-Experten, die in der Lage sind, das Wissen in Standard-Entwicklungsprojekte zu tragen sowie Projekte mit einem starken Cybersecurity-Fokus zum Schutz von Produkten und deren Daten (in der Automobilbranche) abzusichern. Dabei fließt in Projekte immer die Expertise des ServiceXpert-Teams für komplexe Elektronik- und IT-Systeme sowie Diagnose-Know-how ein. Das Team arbeitet intensiv an Cybersecurity Themen von morgen. Mit technologischer Kompetenz und besonderer Kundennähe liefert die ServiceXpert maßgeschneiderten und intelligenten Support und Lösungen im Bereich Elektrik- und Elektronik-Systementwicklung. Die ServiceXpert profitiert zudem als Teil der Cognizant Mobility Gruppe von der IT-Kompetenz der Cognizant.

Teilen

ServiceXpert GmbH
https://servicexpert.de