Pressemitteilung

Wien, 03.06.2019

ÖSTERREICHISCHES KNOWHOW FÜR EUROPÄISCHE CYBERSICHERHEIT IM AUTOMOTIVE MARKT

Sparx Services CE und AIT lancieren neues Cyber-Security-Management-System für den Fahrzeugsektor

Im Februar 2019 lancierte die EU eine Initiative für Cybersicherheit, um Europa in diesem kritischen Bereich voranzubringen. Und bereits jetzt gibt es dazu mit THREATGET ein österreichisches Produkt, das vom AIT Austrian Institut of Technology und Sparx Services CE gemeinsam entwickelt wurde. Es unterstützt Entwickler*innen dabei, Bedrohungen frühzeitig zu erkennen und die damit einhergehenden Risiken rasch abschätzen zu können.

Speziell mit der Einführung der neuen Europäischen Sicherheitsrichtlinie nach ECE Level (UNECE WP29; gilt in der EU und teilweise in Asien) wird Fahrzeugherstellern künftig vorgeschrieben, die Cybersicherheit ihrer Fahrzeugsysteme nachweislich zu überprüfen, um eine Zulassung ihrer Produkte zu erhalten. Hersteller müssen ab nun alle drei Jahre nachweisen, dass sie ein zertifiziertes Cyber-Security-Management-System einsetzen, das alle Stationen vom Fahrzeug-Engineering bis hin zur -Dokumentation berücksichtigt. Mit diesem Cyber-Security-Management-System müssen sie alle Fahrzeugtypen auf Cybersicherheit überprüfen, das mögliche Bedrohungspotential identifizieren und dokumentieren und sicherheitskritische Probleme mit Lösungsvorschlägen adressieren und nachweislich lösen.

THREATGET ermöglicht ECE Konformität

In Voraussetzung für diese Cybersicherheitsüberprüfung ist ein modernes Werkzeug, das die Hersteller überhaupt erst dazu befähigt, ihre Systeme ECE konform zu überprüfen. Peter Lieber, Gründer von Sparx Services CE: „Wir arbeiten mit AIT seit zwei Jahren an dieser Lösung und sind stolz, so rasch damit am Markt auftreten zu können. THREATGET bietet IT-Systemdesignern eine effektive Unterstützung bei Sicherheitsvorkehrungen gegenüber potentiellen Cyberangriffen, sogenannten Threats.“ Die beiden Partner bringen dabei Kompetenzen ein, die sich ideal ergänzen: AIT entwickelt modernste AI Technologien für den Einsatz in einem kritischen Marktsegment und hat über Jahre die THREATGET -Technologie perfektioniert, während Sparx Services CE über profundes Wissen rund um die modellbasierte Systementwicklung mit der Modellierungs-Plattform Enterprise Architect verfügt. Helmut Leopold, Head of Center for Digital Safety & Security am AIT: „Erstmals wird es nun möglich, Safety & Security-Anforderungen schon in der Designphase von Systemen zu berücksichtigen. Damit verschaffen wir europäischen Unternehmen einen beträchtlichen Marktvorsprung in diesem immer wichtiger werdenden Praxisfeld.“

Im Kontext einer stark wachsenden Security Engineering Branche adressiert THREATGET die Zielgruppe der Fahrzeughersteller sowie aller Unternehmen, die Fahrzeugarchitekturen und -

systeme analysieren, um Zertifikate vergeben zu können (z.B. der TÜV) sowie Personen im KFZ-Ausbildungsumfeld.

Artificial Intelligence zur Beherrschung von Komplexität

Die in THREATGET enthaltene Datenbank mit Bedrohungspotential und Lösungsvorschlägen wird derzeit im Rahmen angewandter Forschung und Entwicklung gepflegt und gewartet. Anwender erhalten für das gewünschte Systemmodell (z.B. Fahrzeugplattform) eine Liste möglicher Probleme und daran geknüpfte Lösungsansätze , die dann von einem Security Engineer umgesetzt werden. In diesen manuell gewarteten Katalog fließen auch Updates weiterer Bedrohungskataloge ein, die z.B. von sogenannten Computer Emergency Response Teams (CERT) zusätzlich zusammengestellt werden. Mithilfe von Algorithmen, die sich Künstlicher Intelligenz (AI) bedienen, soll künftig das Update des THREATGET Katalogs um diese externen Bedrohungskataloge automatisch erfolgen. AI hilft auf diese Weise künftig dabei, die Komplexität der immer weiter steigenden Vernetzung unserer Systeme beherrschbar zu halten. THREATGET macht es möglich, dass künftig für alle Hersteller dasselbe Grundsicherheitsprinzip gewährleistet wird. Darüber hinaus soll es für Hersteller von Spezialfahrzeugen (z.B. für den Sicherheitsbereich) auch möglich sein, auf diesem Grundsicherheitsprinzip aufzusetzen und gleichzeitig bestimmte Sicherheitslevel und -regeln in ihren Fahrzeugsystemen manuell zu erweitern.
Der Markt für Lösungen im Bereich Cybersicherheit ist weltweit stark im Wachsen, da einerseits nun endlich gesetzliche Regelungen verbindlich werden und andererseits die Anziehungskraft für kriminelle Angriffe wächst. Europa positioniert sich dabei im Gegensatz zu anderen Ländern sehr klar als sicherheitsbewusster Markt. „Die Rahmenbedingungen in der EU für unsere Lösung sind sehr gut. Daher wollen wir den Markt nun rasch über unser Angebot informieren und den erarbeiteten Wissensvorsprung nutzen“, erklärt Lieber abschließend.

Weiterführende Informationen: https://www.threatget.com (Website in Kürze online) und https://cybersecurity.sparxservices.eu/.

Pressekontakt:

Dipl.-Ing. Rüdiger Maier, M.A.
Leitung Presse- und Öffentlichkeitsarbeit
Sparx Services CE / 4biz.at Consulting GmbH
Tel.: +43-1-9072627-204
ruediger.maier@4biz.at

Mag. (FH) Michael W. Mürling
Marketing and Communications
AIT Austrian Institute of Technology
Center for Digital Safety & Security
T +43 (0)50550-4126
michael.muerling@ait.ac.at I www.ait.ac.at

Mag. Michael H. Hlava
Head of Corporate and Marketing Communications

AIT Austrian Institute of Technology
T +43 (0)50550-4014
michael.hlava@ait.ac.at I www.ait.ac.at
Bildmaterial

Bild 1:
Helmut Leopold (links) und Peter Lieber (rechts) freuen sich über die Markteinführung ihres gemeinsamen Produkts THREATGET – Bild: Wolfgang Franz

Grafik 1:
Diese Abbildung zeigt den Datenfluss zwischen verschiedenen internen Einheiten in einem Fahrzeug. Zu sehen sind die Einheiten "Radar" und "Camera", die Daten aus der externen Umgebung sammeln. Diese werden anschließend durch "Sensor Data Fusion and Decision Making Methoden" verarbeitet. Die Datenübermittlung erfolgt an eine "Telematics", die die Verfolgung des Fahrzeugs steuert. Die Telematik interagiert mit der zentralen " Vehicle Control", um die Geschwindigkeit des Fahrzeugs entweder durch “Brakes“ oder durch “Acceleration“ zu steuern. Das "Infotainment" verbindet sich mit der Telematikeinheit, um dem Fahrer Informationen zur Verfügung zu stellen. Alle Grafiken: AIT

Grafik 2:
THREATGET scannt alle Elemente und Konnektoren im Modell und identifiziert die potenziellen Bedrohungen, die den Sicherheitsmechanismus bedrohen. Im Beispiel werden 46 potenzielle Bedrohungen erkannt. THREATGET fasst anschließend alle erkannten Bedrohungen in einer Benutzeroberfläche zusammen. Diese Schnittstelle hat folgende Bedeutung:
Threats List: Details zu allen erkannten potenziellen Bedrohungen
Threats Reference: Ein Screenshot-Bild der Quelle der erkannten Bedrohungen
Threat Severity: Bewertet die Gefährlichkeit der erkannten Bedrohungen, um auf Grundlage der Parameter sowohl die Auswirkung als auch die Wahrscheinlichkeit zu ermitteln.

Grafik 3:
THREATGET führt eine Risikobewertung durch, um das Risikoniveau aller erkannten Bedrohungen zu berechnen. Diese Risikostufen können über die THREATGET-Risikomatrix zugeordnet werden.

Über Sparx Services Central Europe

Wir sind Experten für die Planung, Gestaltung und Umsetzung von aktivem Enterprise Architecture Management (EAM) auf Basis von Enterprise Architect (Sparx Systems). Als praxisorientierter Sparringpartner begleiten wir Organisationen in softwareintensiven Branchen. Unser Fokus liegt auf der nutzenorientierten Anwendung, Transparenz und Individualität für die EAM Projekte unserer Kunden und deren Beraterökosystem.
Wir setzen auf bewährte Technologien und offene Standards (Archimate, TOGAF, BPMN…), Best-Practices und aktuelle Marktherausforderungen wie Cyber Security Modeling. Wir nutzen dabei auch die neuesten Forschungsergebnisse (z.B. Threatget) des Austrian Institute of Technology (AIT), damit „Security by Design“ Realität wird. THREATGET bietet dem Systemdesigner eine

effektive Unterstützung, um Sicherheitsvorkehrungen gegenüber potenziellen Cyber-Angriffen (threats) in das Design des Systems einzubauen. THREATGET überprüft automatisch Cyber-Sicherheitsbedrohungen sowie Schwachstellen des Systemmodells und schlägt entsprechende Lösungsansätze vor.
https://cybersecurity.sparxservices.eu/

Über AIT

Das AIT Austrian Institute of Technology ist Österreichs größte außeruniversitäre Forschungseinrichtung. Mit seinen acht Centern versteht sich das AIT als hochspezialisierter Forschungs- und Entwicklungspartner für die Industrie. Im Center for Digital Safety & Security werden modernste Informations- und Kommunikationstechnologien (IKT) und Systeme entwickelt, um kritische Infrastrukturen im Kontext der umfassenden und globalen Vernetzung und Digitalisierung sicher und zuverlässig zu gestalten. Im Forschungsbereich Dependable Systems Engineering (DSE) untersuchen Expert*innen seit vielen Jahren die Wechselwirkungen zwischen Safety, Security und Zuverlässigkeit und entwickeln neue Methoden und Tools, um die ganzheitliche Sicherheit von Systemen zu gewährleisten. Die Expert*innen arbeiten federführend an den Industriestandards von morgen mit, z.B. ISO TC 22 (Automobilsektor), ISO TC 299 (Robotik), IEC TC 56 (Dependability), IEC TC 62 (Medizin), IEC TC 65 (Leittechnik für industrielle Prozesse) und AIOTI WG03 (M2M). Diese langjährige Erfahrung und Expertise wird Kunden auch in Form von Schulungen und Beratung zur Verfügung gestellt.