Eine gemeinsame Sprache für die Cybersecurity – Teil I: Einführung und übergreifendes Cybersecurity Management

Welche Ziele, Anforderungen und Richtlinien dienen als Grundlage für ein gemeinsames Verständnis der Cybersecurity-Perspektive bei der Entwicklung von Fahrzeugen im Straßenverkehr? Wie definiert man die Prozesse und managt die Risiken in Übereinstimmung mit ISO 31000?

Der erste Teil bietet eine Einführung in die Thematik und beleuchtet das übergreifende Cybersecurity Management – Ziele, Governance & Culture.

Die mit Spannung erwartete "ISO/SAE 21434 Road Vehicles — Cybersecurity Engineering" liegt seit Juni 2020 als Draft International Standard vor, und ihre endgültige Verabschiedung als internationaler Standard steht kurz bevor. Auch wenn sich noch Änderungen ergeben, ist es sinnvoll, sich mit den Inhalten und Vorgaben auseinanderzusetzen, die das Entwickeln von sicheren Fahrzeugen nicht nur aus der Safety-, sondern nun auch aus der Security-Perspektive abdecken. Bedrohungsanalyse, Risikobewertung, Aktivitäten und Work Products warten darauf, in Angriff genommen zu werden.

Schauen wir uns die Motivation an, die der Norm und dem Dokument zugrunde liegt:

- Sie behandelt die Cybersecurity-Perspektive bei der Entwicklung von elektrischen und elektronischen (E/E) Systemen in Straßenfahrzeugen.
- Sie stellt eine angemessene Berücksichtigung der Cybersecurity sicher.
- Sie soll die Entwicklung von E/E-Systemen dazu befähigen, mit den sich ändernden Technologien und Angriffsmethoden Schritt zu halten.
- Sie stellt Vokabular, Ziele, Anforderungen und Richtlinien als Grundlage für ein gemeinsames Verständnis in der gesamten Lieferkette bereit.
- Sie ermöglicht es Organisationen,
    - Cybersicherheitsrichtlinien und -prozesse zu definieren,
    - das Management von Cybersecurity-Risiken und
    - eine Cybersecurity-Kultur zu fördern

Es geht also auch darum, eine gemeinsame Sprache für Kommunikation und Management von Cybersecurity-Risiken zu etablieren und eine Kultur der Cybersicherheit zu fördern.

Zu einer gemeinsamen Sprache gehören Begriffe, deren Bedeutung allen Ebenen in einem Cybersecurity-Projekt geläufig sein sollte. Voraussetzung dafür ist ein Bewusstsein der Terminologie und der Kultur hinter den Begriffen. Aufgaben und Verantwortlichkeiten erstrecken sich über den Bereich der Entwickler hinaus bis in die Management-Ebene hinein.

Allgemeine Begriffe und Definitionen

Wenn wir in der Security von einem **Threat** sprechen, meinen wir eine Bedrohung, die Verwundbarkeiten (**Vulnerabilities**) ausnutzt, um einen Angriff (**Attack**) auszuführen. Die Risiken (**Risks**) ergeben sich dabei aus der Wahrscheinlichkeit einer erfolgreichen Attacke, gepaart mit dem Schaden, der dadurch entstehen kann.

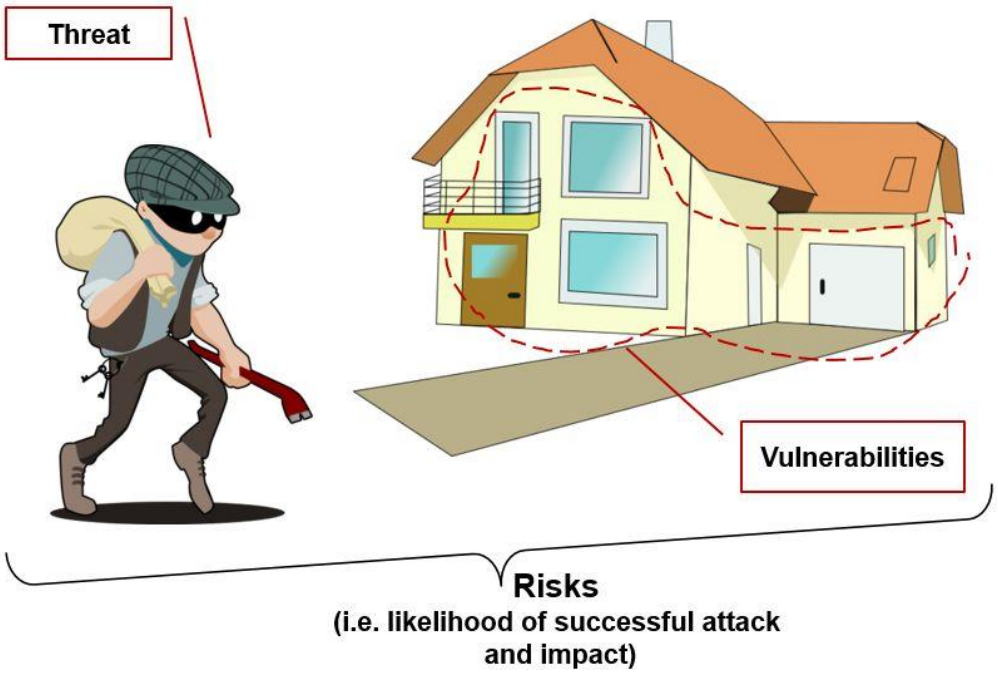

Bild 1: Faktoren der Wahrscheinlichkeit einer erfolgreichen Attacke

Um hier ein bestmögliches und sicheres Szenarium zu schaffen, bedient man sich sogenannter **Cybersecurity Properties**. Ob diese für Ihr Projekt anzuwenden sind, müssen Sie in einer entsprechenden Analyse herausfinden. Für gewöhnlich handelt es sich dabei um eine Kombination mehrerer Attribute.

Zu den wichtigsten schützenswerten Properties (Security Services) gehören:

1. **Integrity** (Integrität von Daten oder Nachrichten)
2. **Confidentiality** (Vertraulichkeit)
3. **Availability** (Verfügbarkeit)
4. **Accountability** (Rechenschaftspflicht)
5. **Authenticity** (Authentizität)
6. **Privacy** (Privatheit)

Evaluation von Cybersecurity-Maßnahmen

Nicht alle in Fahrzeugen verbauten Komponenten sind aus der Sicht der Cybersecurity relevant. Um das festzustellen, hilft ein kurzer Fragenkatalog, mit dem man evaluieren kann, ob die Norm hier greift. Die Fragen beziehen sich dabei jeweils auf die zu untersuchende Komponente.

- Implementiert oder trägt sie zur Fahrzeugfunktionalität durch den Einsatz von E/E-Technologie bei?
- Enthält sie Schnittstellen außerhalb des Fahrzeugs?

- Trägt sie zum sicheren Betrieb des Fahrzeugs bei?
- Enthält sie drahtlos verbundene Sensoren oder Aktoren?
- Implementiert sie Funktionen, die eine Erfassung oder Verarbeitung von benutzerbezogenen Daten erfordern?
- Implementiert sie Fahrzeugfunktionen, die auf vernetzten Komponenten basieren?

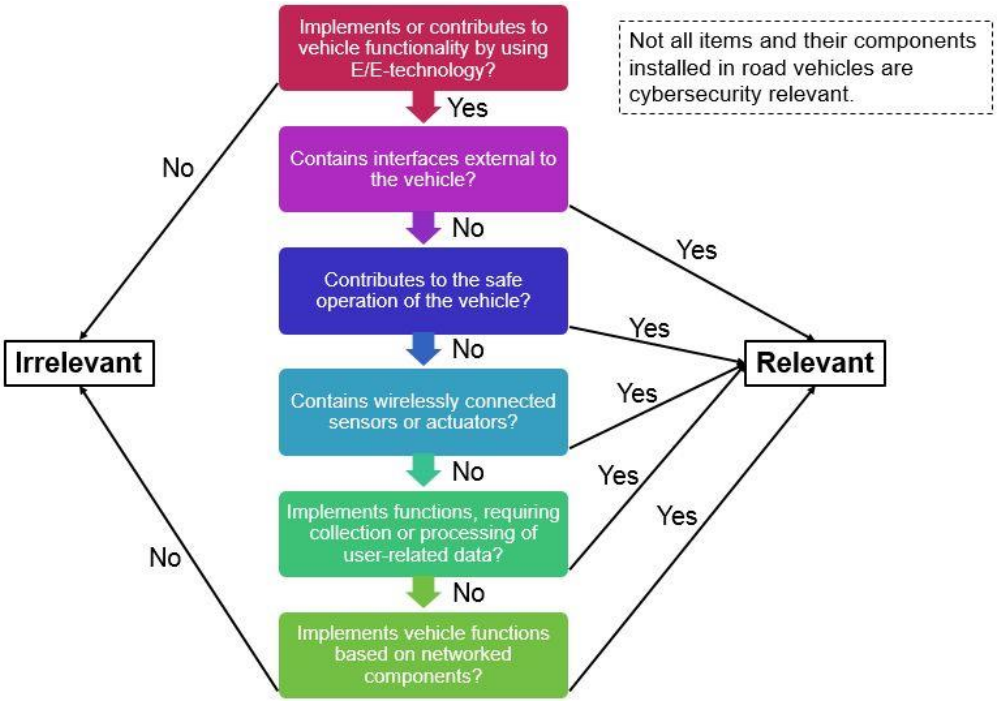

Bild 2: Flussdiagramm zur Bewertung der Cybersecurity-Relevanz

Teil I: Übergreifendes Cybersecurity Management: Ziele, Governance & Culture

Ein übergreifendes Cybersecurity-Management verfolgt eine Reihe von Zielen (**Objectives**):

- eine **Cybersecurity-Richtlinie** sowie organisationsspezifische Regeln und Prozesse definieren
- **Verantwortlichkeiten** und **Befugnisse** zuweisen, die zur Durchführung von Cybersecurity-Aktivitäten erforderlich sind
- die **Umsetzung von Cybersecurity** unterstützen (inkl. Ressourcen und Steuerung der Wechselwirkungen zwischen Cybersecurity-Prozessen und verwandten Prozessen)
- eine **Cybersecurity-Kultur** einführen und pflegen (inkl. Kompetenzmanagement, Awareness-Management sowie ihre kontinuierliche Verbesserung)
- ein **Cybersecurity-Audit** zur Prüfung der Organisation durchführen
- den Austausch von **Cybersecurity-Informationen** managen
- **Management-Systeme**, die Cybersecurity-Aktivitäten unterstützen, einrichten und pflegen
- **Nachweise erbringen**, dass die verwendeten Tools die Cybersecurity nicht beeinträchtigen

Das Cybersecurity-Management ist wie ein Schirm aus Kultur und organisatorischer Führung (**Governance & Culture**), der Cybersecurity ermöglicht, aber auch überwacht.

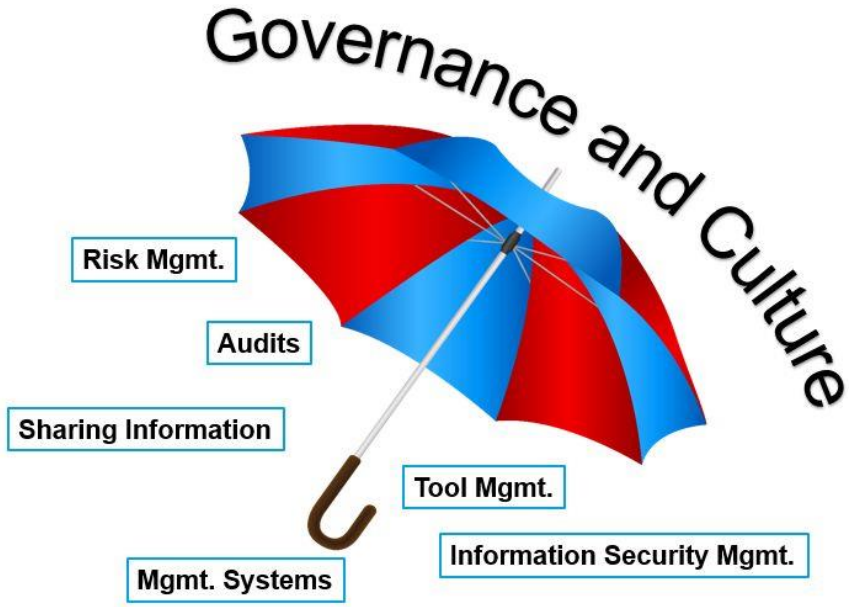

Bild 3: Unter dem Schirm von Governance & Culture

Dabei legt sie Richtlinien (**Policy**) fest, stellt Regeln auf und etabliert Prozesse, indem sie zum Beispiel Guidelines, bewährte Methoden & Templates zur Verfügung stellt. Sie legt Verantwortlichkeiten fest, weist Befugnisse zu (**Responsibilities**) und schafft Ressourcen.

Zusätzlich etabliert Governance & Culture eine Kultur, indem sie Kompetenzen und das Bewusstsein für die Wichtigkeit einer Cybersecurity schafft und einen kontinuierlichen Verbesserungsprozess vorantreibt. Dies geschieht zum Beispiel durch Trainingsprogramme, dem Etablieren von nachvollziehbaren Verantwortlichkeiten (**Traceable Accountability**) und der Betonung von "Security & Safety First". Mit Anreizen gewinnt man Mitarbeiter dazu, die einen Vorteil darin sehen, sich im Bereich der Cybersecurity zu engagieren. Gefördert und belohnt werden sollten in diesem Zusammenhang eine proaktive Einstellung, Vielfältigkeit und Kreativität im Denken sowie die Befolgung von Prozessen.

Risiken, Audits und Informationsmanagement

Das **Risikomanagement** sollte im Einklang mit der ISO 31000 stehen, doch Abweichungen sind grundsätzlich erlaubt. Wird ein **Audit** durchgeführt, so sollte es mit einem Qualitätsmanagement kombiniert werden, um hier effizienter zu arbeiten und keine Ressourcen zu vergeuden. Im besten Fall wird ein Audit nicht nur einmal durchgeführt, sondern erfolgt periodisch und fortlaufend. Dabei ist neben den internen Stellen ausdrücklich ein Blick von außen durch eine extern arbeitende Organisation erwünscht. Auch das **Teilen von Informationen (Sharing)** unterliegt einem kritischen Blick. So sollte festgelegt werden, welche Art von Information unter welchen Umständen überhaupt geteilt werden soll oder darf und wann das nicht erlaubt ist. Wie sieht der Informationsaustausch innerhalb der Organisation aus, und welche Maßnahmen brauchen Sie, um einen sicheren Austausch mit externen Stellen durchzuführen?

Auch die Organisation der unterschiedlichen Managementsysteme darf nicht dem Zufall überlassen werden. Innerhalb des **Qualitätsmanagements** gehören dazu das Änderungsmanagement (**Change Management)**, das **Dokumentationsmanagement**, das **Configuration Management** sowie das Anforderungsmanagement (**Requirements Management**).

Für wen der Begriff neu ist: Im **Konfigurationsmanagement** wird festgelegt und dokumentiert, aus welchen unterschiedlichen Bauteilen und unterschiedlicher Software ein System besteht. Im Fall eines Fehlers kann so die Ursache besser nachvollzogen, überprüft und gefunden werden. Der Umfang des **Änderungsmanagements** in der Cybersecurity besteht darin, Änderungen an Elementen bzw. Komponenten so zu verwalten, dass die betreffenden Cybersecurity-Ziele und -Anforderungen weiterhin erfüllt werden.

Schließlich verdient das **Tool Management** noch besondere Beachtung. Denn auch die Hilfsmittel und Werkzeuge, die man verwendet, um Software zu schreiben und zu testen, können einen negativen Einfluss auf die Security haben. Die korrekte Verwendung der Tools anhand des Benutzerhandbuchs einschließlich Errata, der Schutz vor unbeabsichtigter Verwendung sowie eine Zugriffskontrolle oder Authentifizierung der Benutzer von Software gehören hier dazu.

Ähnlich verhält es sich mit der Informationssicherheit (**Information Security Management**), die ebenfalls einem Cybersecurity-Plan folgen sollte und zum Beispiel die sichere Ablage der Arbeitsprodukte und Dokumente auf einem Fileserver garantiert, der vor unbefugten Zugriffen geschützt ist.

Die bisherigen Punkte, die man unter dem Begriff eines übergreifenden (**Overall**) Cybersecurity Management zusammenfassen kann, stehen über der ganzen Organisation und müssen ständig im Auge behalten werden. Komplettiert wird dies durch das **Project Specific Management,** das bei jedem neuen Projekt gezielt gerichtet eingesetzt wird.

Erfahren Sie im zweiten Teil der Beitragsreihe, was es mit dem projektspezifischen Cybersecurity Management auf sich hat – darunter Ziele, Planung und Assessment.

MicroConsult bietet Ihnen professionelle Trainings und Coachings zu den Themen Safety & Security an – im Live-Online- und im Präsenz-Format.

Weiterführende Informationen

MicroConsult Training & Coaching zum Thema Safety & Security

MicroConsult Fachwissen zum Thema Safety & Security

Alle MicroConsult Trainings & Coachings

Autor

Nach seinem Studium der Elektrotechnik an der Technischen Universität Graz begann die berufliche Laufbahn von **Marcus Gößler** als Field Application Engineer für analoge und digitale Produkte im Bereich Luft-und Raumfahrt. Weitere Applikationsfelder umfassten Audio/Video, portable Systeme und Infotainment im Automobil. Er leitete Applikationsorganisationen in Zentral- und Osteuropa und zeichnete Verantwortung für große Halbleiterhersteller im Vertriebskanal und Marketing. Bei MicroConsult ist er heute als Trainer und Coach im Bereich Embedded Systems tätig, mit Schwerpunkten in sicherheitsrelevanten Anwendungen und Multicore-Bausteinen.