Eine gemeinsame Sprache für die Cybersecurity – Teil II: Projektspezifisches 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 zweite Teil der Beitragsreihe beleuchtet das projektspezifische Cybersecurity Management – Ziele, Planung und Assessment.

Da in jedem Projekt die Zusammenstellung der teilnehmenden Personen und Teams unterschiedlich ist, werden auch die **Verantwortlichkeiten** bezüglich der Cybersecurity-Aktivitäten eines Projekts neu festgelegt. Dazu wird ein **Plan** erstellt, der die Cybersecurity-Aktivitäten einschließlich der Definition der maßgeschneiderten Maßnahmen festlegt.

Das Erstellen eines **Cybersecurity-Cases** liefert den Nachweis für den erreichten Grad an Cybersecurity. Wurde alles Notwendige unternommen, um das System sicher zu bekommen? Ein regelmäßiges **Cybersecurity-Assessment** beurteilt den erreichten Grad an Cybersecurity, was zur Entscheidung führt, ob die Komponente für das **Post Development** freigegeben werden kann.

Verantwortlichkeiten können **übertragen** werden (vorausgesetzt, dies wird kommuniziert und es findet eine Übergabe der relevanten Informationen statt). Beim Zuschneiden der Prozesse (**Tailoring**) werden Tätigkeiten weggelassen oder abweichend ausgeführt. Wenn Aktivitäten zugeschnitten werden, ist immer eine Begründung zu liefern, die beinhaltet, warum die Anpassung angemessen und ausreichend ist. Aktivitäten, die von einer anderen Einheit in der Kette durchgeführt werden, gelten nicht als maßgeschneidert, sondern als verteilte Aktivitäten (**distributed activities**).

Planung und Analyse

Welche Komponenten und Elemente sind weiterhin relevant, welche müssen neu entwickelt werden, und wo verwenden Sie Teile von früheren Projekten? Auf diesen **Cybersecurity-Plan** kann im Projektplan verwiesen werden, oder er wird in den Projektplan inkludiert, wo er unter "Cybersecurity-Aktivitäten" unterscheidbar aufgeführt ist. Auch hier müssen die Verantwortlichkeiten für die Aufrechterhaltung und Verfolgung des Fortschritts von Aktivitäten zugewiesen werden.

Ein solcher Plan zeigt genau auf, wer was wann warum wie macht. Im Detail listet er die Aktivitäten sowie ihre Ziele und Abhängigkeiten zu anderen Zweigen im Projekt auf. Wer ist verantwortlich? Welche Ressourcen werden benötigt? Startpunkt bzw. Endpunkt und die erwartete Dauer sind genauso wichtig wie die Identifizierung der Arbeitsprodukte, die am Ende dabei herauskommen sollen.

Das Wiederverwenden (**Reuse**) von Elementen und Komponenten ist besonders kritisch zu betrachten. Zwar spart es Zeit im Projekt, doch man muss davon ausgehen, dass nichts zu 100% genauso wiederverwendet werden kann, wie es in der Vergangenheit eingesetzt wurde. Irgendwo muss immer eine Änderung eingefügt werden. Eine entsprechende Reuse-Analyse bewertet deshalb anhand genau festgelegter Parameter, ob eine Wiederverwendung den Security-Anforderungen entspricht.

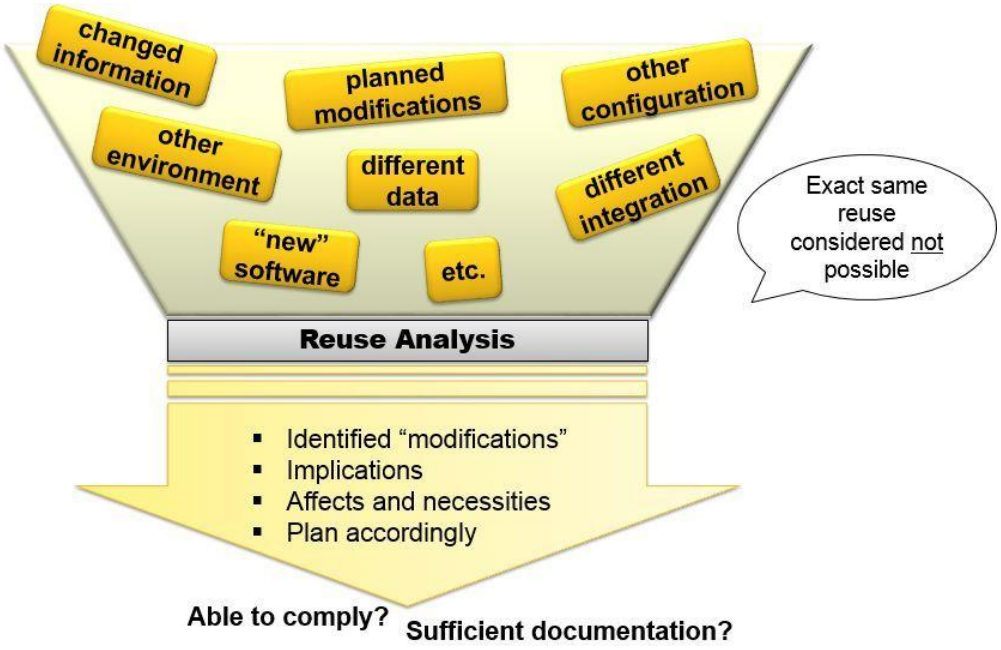

Bild 4: Die Reuse-Analyse bewertet, ob eine Wiederverwendung den Security-Anforderungen entspricht

Out of Context oder Off-the-Shelf?

Unter Umständen arbeitet man zusammen mit anderen Firmen oder Teams an einem größeren Projekt. Diese Projektsituation nennt man **Out of Context.** Man entwickelt für sich, doch man weiß, dass das Produkt am Ende zusammen mit anderen Komponenten in ein größeres Produkt integriert wird. In diesem Fall muss man sich stark auf Annahmen verlassen, die ebenfalls dokumentiert und kontinuierlich abgeglichen und validiert werden, ob sie auch weiterhin zutreffend sind.

Kauft man **Off-the-Shelf**-Komponenten hinzu, dann braucht man Klarheit darüber, ob das Produkt wirklich für Ihren spezifischen Einsatz geeignet ist. Gibt es eine Dokumentation dazu? Müssen Sie es noch anpassen an Ihre Vorgaben und Bedürfnisse? Mitunter können sich Ableitungen ergeben, auf deren Basis man dann weitere Entscheidungen treffen muss. So zum Beispiel, wenn damit zusätzliche Vulnerabilities erzeugt werden und deshalb potentielle Gefahr droht.

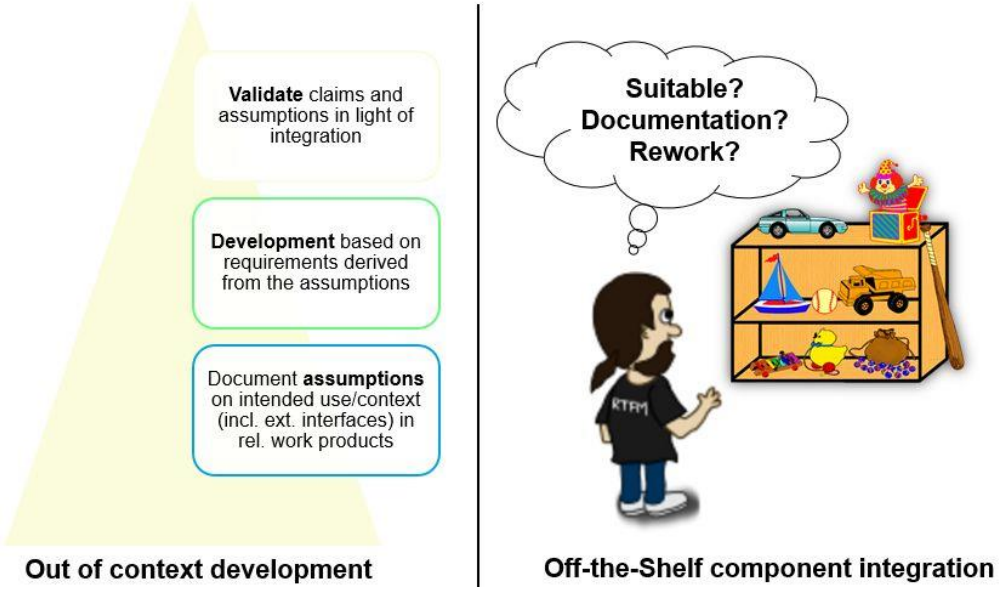

Bild 5: Out of Context oder Off-the-Shelf?

Cybersecurity Assessment: Sind Sie auf dem richtigen Weg?

Während der Entwicklung eines Produktes kann es vorkommen, dass man vom ursprünglichen Weg abkommt. Das kann beabsichtigt sein oder auch unbemerkt passieren. Damit dadurch die Cybersecurity nicht in Gefahr kommt, brauchen Sie geregelte Assessments, die darauf einen prüfenden Blick werfen. Anhand der zur Verfügung stehenden Dokumentation und einem Fragenkatalog kann schnell festgestellt werden, ob alles weiterhin nach Plan läuft.

Das Resultat ist der **Assessment Report**, der beurteilt, ob die verfügbaren Arbeitsprodukte das Vertrauen schaffen, damit der erreichte Grad der Cybersecurity des Teils bzw. der Komponente als ausreichend gilt. Wird befunden, dass man eine Komponente in dem Projekt nicht weiterverwenden kann, dann wird es zurückgewiesen.

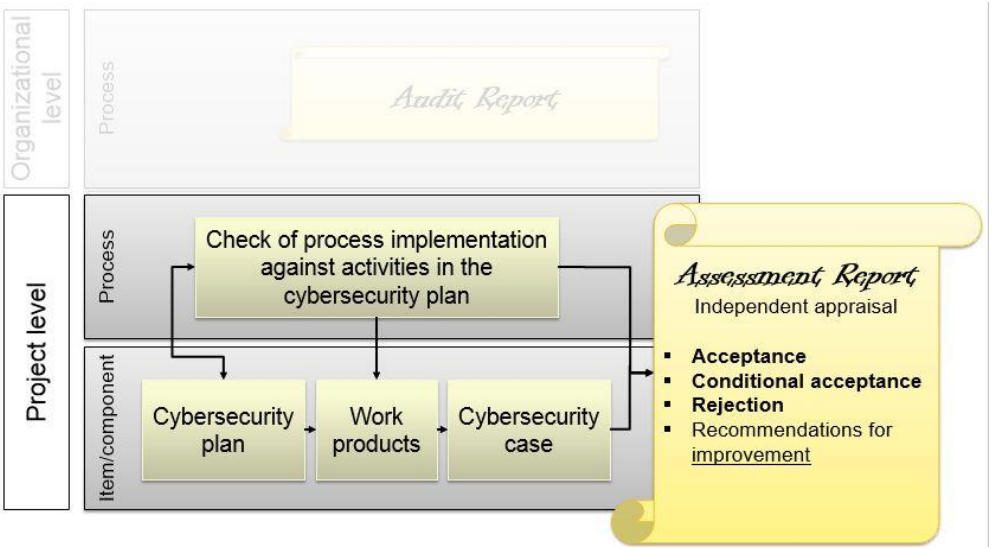

Bild 6: Der Assessment Report beurteilt den Grad der Cybersecurity einer Komponente

Release for Post-Development Report

Zusammen mit dem Cybersecurity Case und dem Assessment Report bieten die **Requirements for post-development** als dritte Säule Anforderungen, die fortlaufend gesammelt werden und darüber Vorgaben liefern, wo in welcher Produktphase nach der eigentlichen Entwicklungsarbeit potentielle Angreifer Schaden anrichten können. Attacken können z.B. auch während der Produktion erfolgen. Die entsprechenden Vorgaben, die man als wichtig empfindet, werden bereits während der Entwicklung gesammelt.

Am Ende steht die Frage: Wird die Cybersecurity mit diesen Vorgaben und Informationen erfüllt? Sind entsprechende Anforderungen für die Post-Development-Phase identifiziert und überprüft? Die Antwort führt dann im besten Falle zur einer expliziten Freigabe, zum Beispiel für den Start der Produktion.

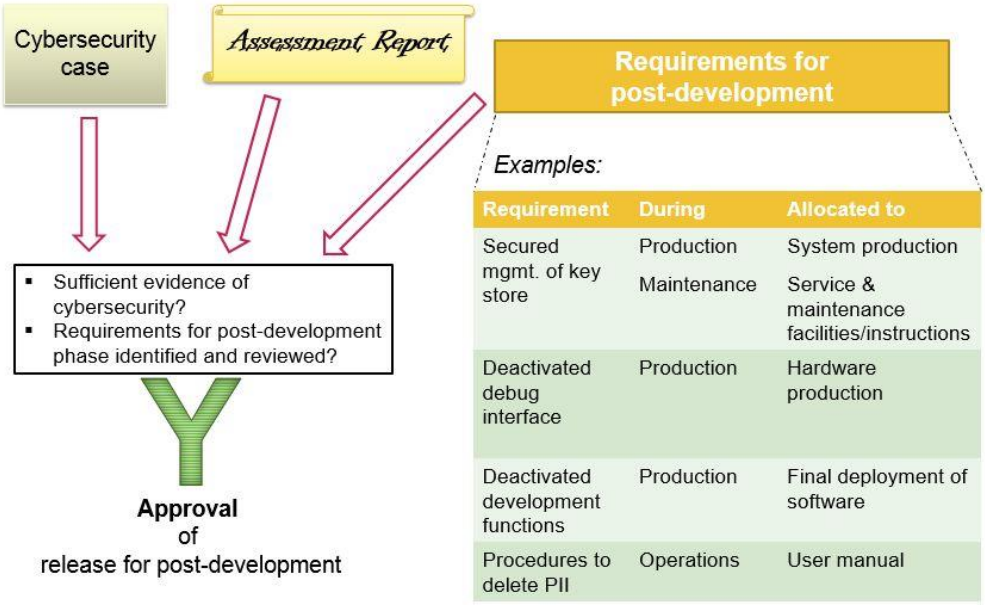

Bild 7: Mit Cybersecurity Case, Assessment Report und Requirements for Post-Development zum Approval of Release for Post-Development

Ein Cybersecurity-Projekt braucht eine solide Grundlage für eine gemeinsame klare Kommunikation. Irrtümer und Missverständnisse können ein solches Projekt von Anfang an gefährden. Wer die Risiken kennt und sie gemeinsam benennen kann, der sichert nicht nur sein Projekt ab, sondern ist auf dem besten Weg, die übergreifende Kultur der Cybersicherheit zu fördern.

Holen Sie sich das richtige Wissen zum Thema Cybersicherheit.

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

Teil 1 dieser Beitragsreihe beleuchtet neben einer Einführung in die Thematik das übergreifende Cybersecurity Management – Ziele, Governance & Culture.

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.