Security-Strategie

2

Zusammenfassung

Cybersecurity ist keine qualitative Eigenschaft oder Zusatzfunktion eines Systems, sondern ein mehrdimensionales Konzept, das sich über den gesamten technischen Bereich, den gesamten Lebenszyklus und die gesamte Organisation eines Unternehmens erstreckt. Das sog. Defence-in-Depth-Prinzip wird in diesem Kapitel nach einer historischen Einordnung als Schutz- und Verteidigungskonzept auf den Automotive-Bereich angewendet, um daraus ein Referenzmodell für eine mehrdimensionale Verteidigungsstrategie zu entwickeln. Hierbei werden die jeweiligen Security-Maßnahmen sowohl den Ebenen der Fahrzeugarchitektur als auch den Verteidigungsstufen zugeordnet. Das Security-Konzept bildet den Anknüpfungspunkt, um das Referenzmodell und damit die Security-Strategie in den Entwicklungsprozess einfließen zu lassen. Eine Aufstellung von Cybersecurity-Best Practices und Designprinzipien, die ebenfalls in das Security-Konzept mit einfließen sollten, dient als Hilfestellung und als Referenz für den Stand-der-Technik.

Moderne Fahrzeuge zählen aufgrund ihrer hohen Anzahl elektronischer Komponenten mit einem gesamten Software-Umfang von oftmals mehr als 100 Mio. Codezeilen sowie aufgrund ihrer verschachtelten E/E-Architektur zu hochkomplexen Systemen. Gleichzeitig decken Standards und Normen noch nicht alle Bereiche der Fahrzeugentwicklung ab, sodass zahlreiche Aspekte OEM- bzw. Zuliefer-spezifisch gelöst werden und deshalb zu inhomogenen Lösungen führen können. Aufgrund dieser beiden Eigenschaften, Komplexität und Inhomogenität, wird angenommen, dass eine 100-prozentige Absicherung gegen die Gefahren von Cyberangriffen mit wirtschaftlich vertretbarem Aufwand nicht erreichbar ist.

Abhilfe schafft ein *risikobasierter Ansatz,* wie er auch im Cybersecurity Engineering Standard ISO/SAE 21434 hinterlegt ist. Im Gegensatz zum reifegradbasierten Vorgehen,

M. Wurm, *Automotive Cybersecurity,* https://doi.org/10.1007/978-3-662-64228-3_2

wo ohne detaillierte Abwägung der jeweiligen Erfordernis bzw. Priorität sämtliche Assets gleichermaßen mit den größtmöglichen Schutzmechanismen ausgestattet werden, sollen beim risikobasierten Ansatz die jeweiligen Wahrscheinlichkeiten und mögliche Auswirkungen der Risiken gegenübergestellt werden, um so eine differenzierte Einordnung der Risiken zu erhalten. So können Gegenmaßnahmen gezielter und effizienter angewendet werden – auch unter Berücksichtigung der unternehmerischen Risiken, die die Produktentwicklung durch mögliche Auswirkungen von Cyberrisiken in sich bergen.

Der *ganzheitliche Lösungsansatz* deckt einerseits das Fahrzeug mit seinen Komponenten als auch die für den gesamten Lebenszyklus erforderliche Infrastruktur ab und umfasst die Bereiche O*rganisatorische Maßnahmen, Sicherer Produktlebenszyklus* sowie *Technische Maßnahmen/Bausteine.*

Der sichere Produktlebenszyklus stellt in Abb. 2.1 für Fahrzeug und Infrastruktur die zentrale Komponente dar, s. Kap. 4.

Organisatorische Maßnahmen schaffen die Rahmenbedingungen und Ressourcen und sorgen für die Nachhaltigkeit der gesamten Security-Strategie. Sie fließen außerdem z. T. in die entsprechenden Lebenszyklusphasen ein, s. Kap. 3.

Die technischen Maßnahmen sichern bestimmte Funktionen und Schwachstellen des Produkts und deren Infrastruktur ab und fließen ebenfalls in die jeweiligen Lifecycle-Phasen ein, s. Kap. 5.

2.1 Mehrschichtiger Ansatz

2.1.1 Historischer Vergleich

Zur Definition der *Verteidigungsstrategie* gegen Cyberangriffe bedient man sich häufig aus dem Wortschatz der militärischen Kriegsführung. *Defence-in-Depth* (dt. Tiefenverteidigung oder elastische Verteidigung) ist eine militärische Strategie, die nach

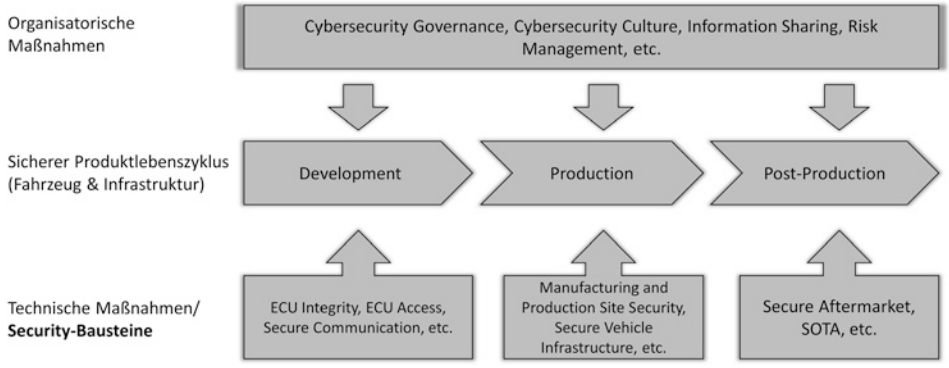

Abb. 2.1 Ganzheitliche Security-Strategie

historischen Überlieferungen bereits von Hannibal erfolgreich in der Schlacht von Cannae angewendet wurde, s. [14].

Diese Verteidigungsstrategie sieht nicht vor, den Angreifer mit der gesamten Stärke an der Frontlinie zu bekämpfen, sondern vielmehr, ihn kontrolliert in das eigene Terrain eindringen zu lassen. Dadurch kann sich das Angriffsmoment verzögern und abschwächen, was einen erfolgreichen Gegenangriff selbst bei zahlenmäßiger Unterlegenheit begünstigen kann. Diese namensgebende Strategie, bei der Verteidigung in die Tiefe zu gehen und mehrere Verteidigungsringe aufzubauen, lässt sich noch besser anhand der Verteidigungsstrategie einer mittelalterlichen Festung erklären. Wir stellen uns dafür eine mittelalterliche Ritterburg mit einem tiefen Ringgraben vor, über die nur eine Zugbrücke führt. Hinter der Zugbrücke trennen jeweils hohe Mauern mit Schießscharten, Wehrgängen und bewachten Toren mit Fallgittern den Zwinger von der Vorburg, bzw. die Vorburg von der Kernburg mit Bergfried. Der Bergfried ist der letzte Rückzugsort für die Burgbewohner und ist nur über einen sehr schmalen und äußert gut bewachten Durchlass zugänglich. Sämtliche Maßnahmen, wie sie in verschiedenen Ausprägungen bei alten Burgen zu finden sind, dienen folgendem Zweck:

- Die Eroberer müssen mehrere Hindernisse und Verteidigungsanlagen überwinden, was einen Angriff und damit eine Eroberung erschwert und in die Länge zieht.
- Die Zugänge zu den jeweiligen Bereichen können (normalerweise) nur über die vorgesehenen Tore und Türen erfolgen, die wiederum bewacht und kontrolliert werden können.

Vergleichbar mit den Eroberungen von Burgen sind auch Angriffe auf eingebettete Systeme in Fahrzeugen typischerweise in mehreren Stufen unterteilt. Wie bei Burgen ist auch bei Fahrzeugen die Zielsetzung, dass das Überwinden jeder Stufe dem Angreifer so schwer wie möglich gemacht werden soll. Das Überwinden der allerletzten Stufe, die Eroberung des Bergfrieds, in dem der Goldschatz oder wahlweise das hübsche Burgfräulein bewacht wird, sollte praktisch unmöglich sein.

Fazit: Um diesen Ansatz für die Abwehr von Cyberangriffen auf Fahrzeuge und deren Infrastruktur zu übernehmen, ist ein mehrstufiges bzw. mehrschichtiges Verteidigungsverfahren (engl. multi-layered defence) zu erschaffen.

2.1.2 Anwendung des Defence-in-Depth-Prinzips

Wie wird das *Defence-in-Depth-Prinzip* als Schutz- und Verteidigungskonzept sinnvoll auf die Strukturen im Automobilbereich angewendet?

Ein früher Beitrag zur Klärung dieser Frage lieferte eine Forschungsarbeit [6], die eine Systematik für die Klassifizierung und Beschreibung von *Anti-intrusion techniques* in technischen Systemen definierten. Die Autoren beschreiben darin sechs Ansätze, um die Systemressourcen eines Computersystems vor einem Cyber-Einbruch zu schützen.

- *Prevention*: Zu diesem Ansatz zählen vorbeugende Maßnahmen, die die Wahrscheinlichkeit für einen Einbruch bzw. Angriff bereits im Vorfeld herabsetzen. Zum Beispiel eine Firewall, die alle eingehenden Verbindungen blockiert, ist eine vorbeugende Maßnahme gegen Angriffe über die externe Netzwerkverbindung.
- *Preemption:* Darunter fallen präventive Maßnahmen gegen mögliche Bedrohungen, sodass es möglichst gar nicht erst zu einem Angriff kommt. Als ein Beispiel nennen die Autoren die Infiltration einschlägiger Informations- und Austauschmedien für Angreifer, um falsche und irreführende Informationen unter möglichen Angreifern zu verbreiten.
- *Deterrence:* Hierbei sind abschreckende Maßnahmen gemeint, die einen Einbruch aus der Perspektive des Einbrechers riskant oder wenig erfolgsversprechend erscheinen lassen. Sie sind vergleichbar mit der militärischen Taktik *Tarnen und Täuschen* und sollen bewirken, dass eigentlich attraktive Ziele für den Angreifer als weniger attraktiv oder gar nicht mehr wahrgenommen werden.
- *Deflection*: Ablenkende Maßnahmen sollen die Einbrecher von den Assets des Systems ablenken und zu einem vermeintlich attraktiven, aber falschen, künstlich erzeugten Ziel leiten. Sog. *Honeypot*-Systeme, die dem Angreifer ein (attraktives) Ziel mit interessantem oder wertvollem Inhalt vortäuschen, sind in dieser Kategorie die am häufigsten genannten Vertreter. Weitere Beispiele sind u. a. die Nutzung von falschen Zugangskonten mit beschränkten Rechten zum Ködern von Angreifern.
- *Detection*: Intrusion Detection Systeme sind Mechanismen, die einen Einbruch erkennen können und übergeordnete Systeme darüber informieren bzw. alarmieren. Beispielsweise kann ein Einbruch erkannt werden, indem Anomalien im Netzwerkverkehr oder im Systemablauf festgestellt werden.
- *Countermeasures:* Darunter fallen alle aktiven Maßnahmen gegen einen erkannten Angriff, beispielsweise Maßnahmen zur Schadensminimierung und Eindämmung möglicher Auswirkungen, indem u. a. bestimmte Funktionen gesperrt werden (Notbetrieb).

Das Defence-in-Depth-Modell von Larson und Nilsson [11] besteht auf vier Stufen: Prevention, Detection, Deflection und Forenics. In ihrer Forschungsarbeit wendeten sie darüber hinaus für jede Stufe konkrete technische Maßnahmen an:

- Ein sicheres Updateverfahren als präventive Maßnahmen, um das Einschleusen manipulierter Software zu verhindern,
- ein Intrusion Detection System als Mechanismus zum Erkennen eines Einbruchs,
- ein Honeypotsystem als ablenkende Maßnahme und
- eine Infrastruktur zur forensischen Untersuchung stattgefundener und erkannter Angriffe.

Le et al. [9] zeigen aus verschiedenen Sichtweisen den aktuellen technischen Stand und verschiedene Forschungsaktivitäten für Security-Mechanismen. In ihrer dargestellten

Sichtweise „Stage view“ sind die Security-Mechanismen anhand der Defence-in-Depth-Stufen Prevention, Detection, Deflection und Response zugeordnet – in Anlehnung an das von Nilsson und Larson vorgestellte Prinzip. Sie beließen es dabei nicht beim linearen Stufenmodell von Nilsson und Larson. Genauer gesagt erweiterten sie die Möglichkeiten des Modells, indem zusätzlich zum Stufenmodell des Defence-in-Depth-Prinzips auch eine Zuordnung zu verschiedenen Architekturebenen innerhalb („In-vehicle systems“) und außerhalb („VANETs“) des Fahrzeugs erfolgt. Dies bietet den Vorteil, dass die Verteidigungslinien nicht nur auf die einzelnen Angriffsstufen, sondern auch auf die Architekturebenen verteilt werden können. Auf diese Weise wird der Grundstein für die Planung eines mehrdimensionalen Verteidigungskonzepts gelegt, s. Abschn. 2.2.

Dieses Modell ermöglicht außerdem eine genauere Analyse und Bewertung der Angemessenheit und Notwendigkeit der einzelnen Security-Bausteine. So kann etwa auf bestimmte Maßnahmen verzichtet werden, falls das System über entsprechende physische oder logische Redundanzen und Plausibilisierungsmöglichkeiten verfügt. Die Anpassung an das konkrete Angreifermodell des jew. Systems und dessen Kontext spart Kosten und Entwicklungskapazitäten.

Darüber hinaus ist auf diesem Wege die Identifikation von Lücken im Verteidigungskonzept möglich. Sind auf allen Ebenen genügend geeignete präventive Maßnahmen vorhanden? Wurde das zugrunde liegende Prinzip von Defence-in-Depth eingehalten und das Verteidigungs- und Schutzkonzept so gestaltet, dass der Angreifer möglichst viele Verteidigungslinien überwinden muss? Dementsprechend lässt sich beispielsweise in der Konzeptphase bereits leicht erkennen, ob und welche Detektionsmechanismen auf der ECU-Ebene oder auf der Netzwerkebene eingeplant sind.

Diese Prüfungen können sowohl initial, in der Konzeptphase, als auch zu späteren Zeitpunkten innerhalb der Produktlebenszeit durchgeführt werden. Sie schaffen die Möglichkeit, das Verteidigungskonzept über die gesamte Produktlebensdauer hinweg an die sich stetig verändernde Bedrohungslage anzupassen.

Die Umsetzung des Defence-in-Depth-Prinzips birgt allerdings auch Nachteile. Bildlich gesprochen: Indem die Anzahl der Verteidigungslinien erhöht wird, verlängert sich auch der Weg, den eine Nachricht durch das Fahrzeug nehmen muss. Bezogen auf die Technik bedeutet das, dass zusätzliche Securityfunktionen den Ressourcenbedarf im Allgemeinen und die Laufzeit für kryptographische Funktionen im Speziellen erhöhen und zu Verzögerungen im Informationsfluss führen. Insbesondere für Echtzeitanwendungen kann diese Auswirkung problematisch sein. Außerdem führen zusätzliche Securityfunktionen auch zu zusätzlichen Aufwänden in der Entwicklung, im Test und in der Wartung. Das Erzielen eines sorgfältig ausgewogenen Verhältnisses aus Schutzbedarf, Angriffswahrscheinlichkeit und Kosten ist anzuraten. Falls die Kosten für den Schutz eines Assets höher sind als der eigentliche Wert des Assets wurde vermutlich über das Ziel hinausgeschossen.

Ein überzeugendes Beispiel für eine schlecht angepasste Securitystrategie stammt aus dem Energiesektor. Die elektronischen Steuerungen von Windkraftanlagen werden

mittels sog. SCADA-Systeme (Supervisory Control and Data Acquisition, dt. Überwachung, Steuerung und Datenerfassung) gewartet und gesteuert. Die Steuerungen der einzelnen Anlagen kommunizieren dabei häufig über eine Ethernet-Verbindung mit den zentralen SCADA-Rechnern. Ohne Berücksichtigung der herrschenden Umgebungsbedingungen werden für eine Verteidigungsstrategie sowohl Fernangriffe, in diesem Fall über die Ethernet-Verbindung, als auch lokale, physische Angriffe auf die elektronische Steuerung berücksichtigt. Unter Berücksichtigung des Systemkontextes einer Windkraftanlage innerhalb eines Offshore-Windparks wird jedoch schnell klar, dass in rund 50 m Höhe und mehrere Kilometer vom Festland entfernt der physische Zugang zu den Steuerungen schwierig und aufwendig und deshalb unwahrscheinlich wird. Kurzum, eine angepasste Securitystrategie wird in diesem Kontext den Schwerpunkt auf die Absicherung der Backend-Systeme und Ethernet-Verbindungen mit den Offshore-Anlagen legen.

2.2 Referenzmodell für eine mehrdimensionale Verteidigungsstrategie

Wie im vorherigen Abschnitt skizziert, führt die Anwendung des Defence-in-Depth-Prinzips auf die verschiedenen Ebenen der Fahrzeugarchitektur zu einer mehrschichtigen bzw. unter Berücksichtigung der Tiefenwirkung zu einer mehrdimensionalen Verteidigungsstrategie.

In diesem Abschnitt wird ein Referenzmodell vorgestellt, das sowohl die mehrdimensionale Verteidigungsstrategie umsetzt als auch die oben definierten, ganzheitlichen und risikobasierten Lösungsansätze berücksichtigt.

Im vorgestellten Referenzmodell, s. Abb. 2.2, sind auf der vertikalen Achse die Ebenen der Fahrzeugarchitektur aufgelistet – von außen nach innen sortiert:

- *Infrastruktur:* beinhaltet alle Infrastruktur- und Backendkomponenten, die mit dem Fahrzeug kommunizieren sowie systemübergreifende Funktionen, die für die Security des Fahrzeugs eine Rolle spielen
- *Fahrzeug:* berücksichtigt alle Außenschnittstellen des Fahrzeugs sowie alle Funktionen, die für die Gesamtintegrität des Fahrzeugs sorgen
- *Netzwerk:* beinhaltet das fahrzeuginterne Kommunikationsnetzwerk
- *ECU:* beinhaltet alle ECU-internen Funktionen, sowie deren Außenschnittstellen

Auf der horizontalen Achse sind die Stufen der Defence-in-Depth-Tiefenverteidigung aufgeführt: in der linken Spalte die präventiven Maßnahmen, in der mittleren Spalte die Maßnahmen zum Erkennen eines Angriffs und in der rechten Spalte stehen die Maßnahmen zum Ablenken und Abschwächen der Auswirkungen eines Angriffs, vgl. [9].

Ebenen der Fahrzeugarchitektur				
	Infrastruktur	Secure Backend, Key Management, Production Site Security, Secure OTA-Update, Aftermarket Protection	Intrusion Detection System (Backend)	Redundancy/ Backup Systems
	Fahrzeug	Firewall, Secure Backend Communication, Secure V2X Communication	Intrusion Detection System (Fzg)	
	Netzwerk	Sichere Buskommunikation, Netzwerk-Segmentierung		Netzwerk-Segmentierung, Honeypot
	ECU	Secure Boot/Programming, Hardening, Secure ECU-Access, Hardware Security Support	Runtime Manipulation Detection, Control Flow Integrity	Secure Execution Environment/ Virtualisierung
		Prävention	**Erkennung**	**Ablenkung u. Abschwächung**
	Verteidigungsstrategie			

Abb. 2.2 Referenzmodell für die Anwendung der Verteidigungsstrategie auf die Ebenen der Fahrzeugarchitektur

Prävention Zur Prävention von Angriffen sollen auf der Infrastrukturebene Maßnahmen zur Absicherung des Backends und der Produktionsumgebung getroffen werden. Außerdem sollen systemübergreifende Funktionen, d. h. Funktionen wie Schlüsselmanagement, Update-Over-the-Air und Aftermarketzugang, die sich sowohl über Fahrzeug- als auch Infrastrukturkomponenten erstrecken, geschützt werden.

Auf der Fahrzeugebene sollen sämtliche Außenschnittstellen, wie etwa Verbindungen zum Backend und die V2X-Kommunikation, abgesichert werden. Mittels einer Firewall soll der Zugriff von außen grundsätzlich beschränkt und kontrolliert werden.

Auf der Netzwerkebene ist dafür zu sorgen, dass der fahrzeuginterne Datenaustausch zwischen den ECUs, Aktoren und Sensoren abgesichert ist, d. h. dass die interne Kommunikation nicht als Angriffspunkt ausgenutzt werden kann. Des Weiteren soll die Topologie des Kommunikationsnetzwerks etwa durch eine geeignete Segmentierung hinsichtlich ihrer Security-Eigenschaften optimiert werden.

Auf der ECU-Ebene sind verschiedene Maßnahmen zu treffen, um zum einen den Zugriff auf die ECU zu kontrollieren und zum anderen um die Integrität der ECU unter allen Umständen sicherzustellen. Hierzu zählen insbesondere Funktionen, die die Software-Integrität verifizieren und die besonders schützenswerte Daten wie kryptographische Schlüssel vor unbefugtem Zugriff und vor Manipulation schützen. Die Zuordnung des HSMs in diese Kategorie ist ambivalent und deshalb diskussionswürdig. Einerseits stellt ein Hardware Security Modul, bzw. allgemein formuliert eine sichere und vertrauenswürdige Ausführungsumgebung mit sicherem Schlüsselspeicher, eine präventive Maßnahme dar, weil damit der Zugriff auf schützenswerte Daten verhindert wird. Andererseits zählen SEE/TEE auch zu den abschwächenden Maßnahmen, weil ein Angriff oftmals nicht direkt auf das HSM abzielt, sondern über eine Lücke im Gesamtsystem (z. B. in der Applikationssoftware oder im Diagnosestack) beginnt und im

weiteren Verlauf des Angriffspfades die Integrität und Vertraulichkeit des HSMs angreift. Eine SEE/TEE kann umgeben von einer kompromittierten Umgebung dann immer noch die „sichere Welt“ weitestgehend am Laufen halten und den Angriff somit abschwächen. Zusätzlich kann ein HSM beispielsweise durch Maßnahmen wie das Sperren des Schlüsselspeichers und das Verweigern von Kryptofunktionen auf einen erkannten Angriff reagieren. Die Trennung schützenswerter Software vom Restsystem ist somit sowohl eine präventive Maßnahme, kann im Verlauf eines Angriffs auf das Restsystem jedoch auch für die Kontrolle ablenkender und abschwächender Maßnahmen genutzt werden.

Erkennung Zum Erkennen von Angriffen werden sowohl im Backend als auch im Fahrzeug sog. *Intrusion Detection Systeme* verwendet. Auf der ECU-Ebene prüfen darüber hinaus Mechanismen wie *Runtime Manipulation Detection* und *Control Flow Integrity* zur Laufzeit die Systemintegrität und können somit auch Angriffsversuche erkennen.

Ablenkung und Abschwächung Zum Ablenken von Angriffen dienen im Wesentlichen sog. *Honeypot-Systeme,* die die Angreifer in ein künstlich erzeugtes System locken sollen. Von hier aus können Angreifer keinen Schaden auf das reale System ausüben und die aufgezeichneten Aktivitäten der Angreifer können zur forensischen Analyse herangezogen werden, um die Fähigkeiten und das Verhalten der Angreifer zu untersuchen. Abschwächende Maßnahmen dienen dazu, die Auswirkungen eines zumindest teilweise erfolgreichen Angriffs begrenzt zu halten, um ein Mindestmaß an Funktionalität und Kontrolle zu erhalten. Auf Gesamtsystemebene (Infrastruktur und Fahrzeug) helfen hierbei Redundanz- und Backupkonzepte. Auf Netzwerkebene soll eine Segmentierung der Netzwerktopologie die Ausbreitung eines Angriffs über Zonen- bzw. Domänengrenzen hinweg erschweren. Auf der ECU-Ebene verhindert die Segmentierung und Isolation sicherheitsrelevanter Software und Daten den Zugriff von möglicherweise kompromittierten Gastgebersystemen.

Zusammenfassend wird festgehalten, dass das vorgestellte Referenzmodell sowohl die Fahrzeugarchitektur berücksichtigt als auch die Verteidigungsstrategie umsetzt und als Ergebnis eine Aufstellung aller erforderlichen Securitybausteine als Beitrag für das Securitykonzept, s. folgender Abschnitt, liefert.

Die zugrunde liegende Verteidigungsstrategie ist:

- *risikobasiert*, weil davon ausgegangen werden muss, dass weiterhin Lücken bestehen und kein hundertprozentiger Schutz erreicht werden kann, und
- *ganzheitlich,* weil zusätzlich zur gesamten Fahrzeugarchitektur auch die relevante Infrastruktur für die Verteidigungsstrategie einbezogen wird.

2.2.1 Anpassungsfähigkeit an unterschiedliche Bedrohungsszenarien

Fahrzeuge und die zugehörige Infrastruktur stellen mit ihren vielen verschiedenen Assets und Angriffspunkten ein relativ komplexes System dar, was zur Folge hat, dass man es nicht mit einer oder einigen wenigen Bedrohungen und den verbundenen Risiken zu tun hat, sondern mit vielschichtigen *Bedrohungsszenarien*, s. Abschn. 1.2.3.

Unterschiedliche Bedrohungsszenarien kommen durch mehrere Variablen, die auch im Rahmen der TARA für die Bewertung von Bedrohungen und Risiken herangezogen werden, zustande.

Zunächst wird das Potenzial einer Bedrohung u. a. anhand der zugeordneten Angreifertypen, der verwendeten Angriffsvektoren bzw. Einstiegspunkte (engl. entry points) sowie des erforderlichen Gelegenheitsfensters ermittelt.

Skript-Kiddies, Laymen und Thrill-Seekers, die mit einfacheren Mitteln und mit eher geringem Eigenrisiko versuchen, Fahrzeuge und Automotive-Infrastrukturen anzugreifen, sind (zunächst) die wahrscheinlicheren Angreifer als *Nation-States* und cyberkriminelle Organisationen, die etwa mit geopolitischer Taktik, zur Kriegsführung oder für ihren eigenen Profit versuchen, Fahrzeuge anzugreifen. Die erstgenannte Gruppe wird zudem mit höherer Wahrscheinlichkeit Fernangriffe durchführen und infolgedessen die Internetverbindungen und die Funkschnittstellen des Fahrzeugs (BT, WiFi, Mobilfunk) als Einstiegspunkte wählen. Physische Angriffe sind deshalb nicht weniger wahrscheinlich, sie erfordern allerdings den zumindest zeitlich beschränkten Zugriff auf ein Fahrzeug. Das Gelegenheitsfenster ist bei Angriffen auf Internetverbindungen praktisch unendlich und zudem leicht skalierbar, indem weltweit verteilte Ressourcen (und Komplizen) eingebunden werden können. Angriffe auf die Funkschnittstellen erfordern zumindest die Anwesenheit des Angreifers in Empfangsreichweite.

Darüber hinaus erfolgt im Rahmen der TARA die Bewertung der erwarteten Auswirkungen eines Angriffs anhand der Kategorien Verfügbarkeit, Sicherheit (Safety), Privacy und des möglichen finanziellen Schadens.

Auch bezüglich dieser Variablen können mehrere verschiedene Bedrohungsszenarien entstehen, denen mit unterschiedlichen Strategien entgegengewirkt wird. Beispielsweise kann das Erdulden (geringer) finanzieller Schäden durch äußerst seltene oder unwahrscheinliche Angriffe für ein Unternehmen günstiger sein als die kostenintensive Implementierung und Wartung spezieller Securitybausteine. Auch der Versuch, mittels ausgetüftelter Schutzmechanismen auch unter widrigsten Umständen die Verfügbarkeit aller Systemfunktionen eines Fahrzeugs aufrecht zu erhalten, stehen zum Teil im Widerspruch zu den hocheffizienten und kostengünstigen Methoden, die etwa durch mutwillige Sachbeschädigung an einem Fahrzeug erreicht werden.

Derartige Abwägungen sind nicht allgemeingültig und müssen von Fall zu Fall, individuell für jede Produktgruppe neu bewertet werden. In jedem Fall dient das oben vorgestellte Referenzmodell als Grundlage für die Aufteilung, Planung und Priorisierung

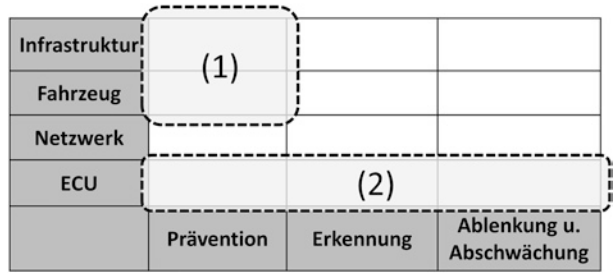

Abb. 2.3 Beispielszenario mit priorisierten Securitybausteinen

mehrerer Bedrohungsszenarien. Auf diese Weise werden den jeweiligen Bedrohungsszenarien die erforderlichen Securitybausteine zugeordnet. Es bietet darüber hinaus den nötigen Überblick, um zu verhindern, dass konzeptuelle Lücken im Securitykonzept unentdeckt bleiben.

Beispiel

Beispielszenario mit priorisierten Securitybausteinen, s. Abb. 2.3:

- In folgenden, beispielhaften Szenario wird angenommen, dass es oftmals nicht möglich ist, das gesamte Securitykonzept von Beginn an lückenlos und fehlerfrei zu implementieren. Deshalb wird eine *Priorisierung* der zu implementierenden Securitybausteine und damit deren Reihenfolge der Implementierung festgelegt. Welche Bausteine sind aber wichtiger als andere? In der Produktentwicklungsphase sind physische, lokale Angriffe (durch externe Angreifer) weniger wahrscheinlich, weil die Gelegenheitsfenster und die physischen Zugriffsmöglichkeiten nicht vorhanden sind. Fernangriffe auf das Fahrzeug und auf die Backend-Infrastruktur sind jedoch bereits möglich. Die höchste Priorität bekommen demnach präventive Maßnahmen gegen Fernangriffe (1), die zur Absicherung aller fahrzeugexternen Schnittstellen und Backend-/Internetverbindungen dienen.
- Die zweithöchste Priorität erhält die komplette Absicherung einzelner, kritischer ECUs (2) wie etwa Domain-Controller, Gateways, Head-Units oder Telematikeinheiten. Deren Integrität wird in diesem Beispiel höher bewertet als der Schutz von weniger kritischen Komponenten wie die Steuerung der Fensterheber. ◀

2.3 Security-Konzept

Wie wird die Security-Strategie und das davon abgeleitete Referenzmodell, sowie die Best-Practices mit dem *Security-Konzept* verknüpft? Was ist das Security-Konzept überhaupt?

In ISO21434 [7] ist das Security-Konzept definiert als die Zusammenfassung der Cybersecurity-Anforderungen zur Erfüllung der *Cybersecurity-Goals* und deren Zuordnung zu (den Elementen der) Security-Architektur.

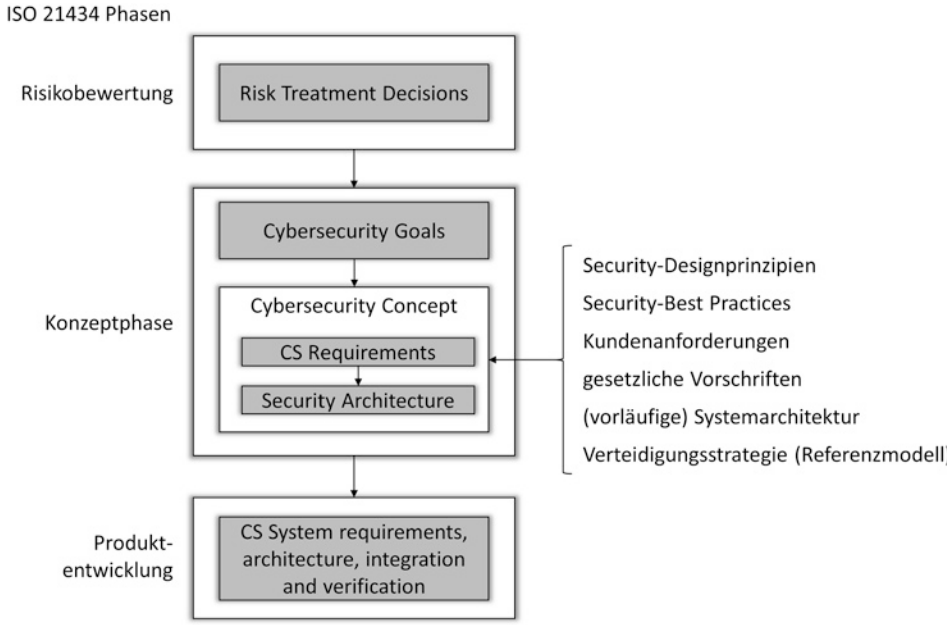

Abb. 2.4 Security-Konzept im Kontext des Cybersecurity-Engineeringprozesses

Die Cybersecurity-Anforderungen werden einerseits von den Cybersecurity-Goals und diese wiederum von den *Risk Treatment Decisions* abgeleitet, s. Abb. 2.4. Andererseits sollten bereits in der Konzeptphase Security-Designprinzipien, Best Practices, Kundenanforderungen und gesetzliche Anforderungen für die Definition des Security-Konzepts einbezogen werden. In der darauffolgenden Produktentwicklungsphase werden die oben genannten Quellen erneut herangezogen, allerdings auf einer detaillierteren Abstraktionsebene und zum Verfeinern der Anforderungen.

Als Grundlage für die Security-Architektur dienen wiederum die vorläufige Systemarchitektur sowie der gewählte Lösungsansatz für die Verteidigungsstrategie. Für den sensiblen Schritt in der Konzeptphase, der Zuordnung von Security-Anforderungen zu den Komponenten des Systems oder dessen Infrastruktur, dient das oben vorgestellte Referenzmodell als Gerüst, bietet Orientierung und ermöglicht einen systematischen Abgleich mit ähnlichen Systemen.

2.4 Best Practices

Die Gemeinschaft der Fahrzeughersteller steht zusammen mit ihren Zulieferern weltweit gleichermaßen vor der Herausforderung, ihre Produkte und Unternehmen vor den Risiken von Cybersecurity-Angriffen zu schützen. Um das Rad nicht jedes Mal neu zu

erfinden, erscheint ein Erfahrungsaustausch über Erfolge und Misserfolge sowie das Schaffen und Austauschen einer gemeinsamen Wissensbasis ratsam.

Best Practices, auf Deutsch etwa *beste Vorgehensweisen* oder *Methoden,* bezeichnet die Zusammenstellung aktueller Empfehlungen und den Stand der Technik für eine bestimmte Thematik. Best Practices führen durch die komplexen Problemstellungen, liefern dafür mögliche Lösungswege und geben branchenübergreifende Richtlinien vor. Sie geben einerseits Orientierung, andererseits aber auch einen Leitfaden bzw. eine untere Messlatte, die nur in begründeten Fällen unterschritten werden sollte.

Eine Übersicht der wichtigsten Quellen für Automotive Cybersecurity Best Practices:

- ISO/SAE 21434 – Road vehicles – Cybersecurity engineering, s. [7]
- SAE J3061 -Cybersecurity Guidebook for Cyber Physical Vehicle Systems, s. [12]
- Automotive Information Sharing And Analysis Center (Auto ISAC) – Automotive Cybersecurity Best Practices, s. [2]
- National Highway Traffic Safety Administration (NHTSA), U.S. Department of Transportation – Cybersecurity Best Practices for the Safety of Modern Vehicles, s. [10]
- Agentur der Europäischen Union für Cybersicherheit (ENISA) – Good Practices for Security of Smart Cars, s. [1]
- European Automobile Manufacturers Associations (ACEA) – Principles of Automobile Cybersecurity, s. [5]
- Department for Transportation UK (DfT) – Principles of cyber security for connected and automated vehicles, s. [3]

2.4.1 Security-Designprinzipien

Security by Design Die weitreichenden Auswirkungen von Securityrisiken macht es notwendig, die Disziplin *Security* in allen Phasen des Produktentwicklungsprozesses und Produktlebenszyklus zu berücksichtigen. Insbesondere am Beginn, in der Designphase, gilt es, mögliche Bedrohungen durch Cybersecurity-Angriffe sowie die daraus resultierenden Risiken frühzeitig zu erkennen. So können geeignete Maßnahmen zur Reduzierung der Angriffsoberfläche des Systems von Anfang an in den Entwicklungsprozess einfließen. Security nachträglich zu integrieren oder am Ende „anzuflanschen“ ist in der Regel teuer, kompliziert, fehleranfällig und deshalb auch unsicher, weil sich so die Gefahr für Schwachstellen erhöhen.

Durch die Einführung und konsequente Umsetzung eines Security Engineering Prozesses sowie dessen Anbindung an den Produktenwicklungsprozess, s. Kap. 4, wird außerdem sichergestellt, dass verschiedene empfohlene und bewährte Methoden für die Entwicklung sicherer Systeme in die Designentscheidungen einfließen. ISO 21434 und SAE J3061 führen beispielsweise die Anwendung des sog. *Least Privilege Prinzips* und

die durchgängige Absicherung aller Schnittstellen als gängige und empfohlene Praktiken an.

Security by Default Sämtliche Voreinstellungen sollten so gewählt sein, dass sich das System in einem möglichst sicheren (im Sinne von Security) Zustand befinden. Zum einen wird so sichergestellt, dass Software-Funktionen mit sicheren Konfigurationen initialisiert werden. Zum anderen werden auf diese Weise bestimmte Funktionen und Schnittstellen standardmäßig deaktiviert und somit die Angriffsoberfläche des Systems verkleinert. Dieses Prinzip beinhaltet auch ein sog. Secure Fallback, den Sprung auf eine sichere Rückfallebene – insbesondere in einem Fehlerfall.

Secure Access Mehrere Mechanismen wie Authentifizierung und Autorisierung kontrollieren und beschränken Zugänge und Zugriffsmöglichkeiten auf die Dienste und Daten des Systems. Ein Einhalten des *Least Privilege Prinzips* führt dazu, dass alle Benutzer ausschließlich mit den Berechtigungen ausgestattet sind, die für ihre Aufgabe bzw. Rolle zwingend erforderlich sind. Berechtigungen, die nicht benötigt werden, müssen den jeweiligen Benutzern wieder entzogen werden. Regelmäßige Audits überprüfen die Rechtevergabe und passen sie ggf. an. Eine Logging-Funktion speichert alle Zugriffe in einem manipulationssicheren Speicher ab.

In Bezug auf den Schutz vor Insider-Angriffen wird häufig der römische Dichter Juvenal mit der folgenden Frage zitiert: *„Quis custodiet ipsos custodes?“* (dt. Wer bewacht die Wächter?), s. Juvenal, Satiren VI [13]. Übertragen auf die Cybersecurity-Bedrohungen, die im Automotive-Bereich möglich sind, beschreibt Juvenal damit das Problem des möglichen Missbrauchs von Rechten durch deren legitimen Inhaber. Besonders die Rechte auf kritische Funktionen und Daten, wie beispielsweise das Key Management, müssen sorgfältig kontrolliert werden.

Diehl empfiehlt hierfür zwei Gegenmaßnahmen, s. [4]: Zum einen sollten Berechtigungen sorgfältig voneinander getrennt werden und in verschiedene Rollen, die jeweils für sich keinen kritischen Missbrauch ermöglichen, aufgeteilt werden. Ein Anhäufen mehrerer kritischer Berechtigungen zu „Superuser“-Rollen soll vermieden werden. Zum anderen sollten Zugriffe auf kritische Dienste bzw. Daten stets protokolliert werden und die Protokolle sollten auch regelmäßig ausgewertet und nach Hinweisen für Missbrauch durchsucht werden.

Security-Architektur Zur Erhöhung des Angriffsschutzes und der Ausfallsicherheit sollte die E/E-Architektur, genauer gesagt die physische Architektur, segmentiert werden, d. h. die ECUs sollten voneinander getrennt und jeweils einer geeigneten Domäne, zugeordnet werden, s. Abschn. 5.3.1. Domänenübergreifende Kommunikation sollte zwar ermöglicht jedoch auch beschränkt und kontrolliert werden. Diese Segmentierung und Isolierung führt einerseits zu einer erhöhten Ausfallsicherheit des Gesamtsystems, weil sich Fehler in der Regel nur auf die betroffenen Domänen auswirken. Andererseits werden auch Security-Risiken in einer Domäne auf eben diese

beschränkt, d. h. einem Angreifer wird es erschwert, seinen Angriffspfad über die Domänengrenzen hinaus fortzuführen.

Das Konzept der Segmentierung bzw. Isolation lässt sich auch auf die ECU-Ebene übertragen. Das Schaffen einer sicheren Domäne innerhalb einer ECU bzw. innerhalb eines SoC oder Mikrocontrollers führte überdies zur Entwicklung von Hardware-unterstützten, sicheren Laufzeitumgebungen wie *HSMs* oder *TrustZones,* s. Abschn. 5.1.4.

Kontrolle der Schnittstellen Sämtliche Schnittstellen müssen kontrolliert bzw. abgesichert werden, insbesondere Test- und Entwicklungsschnittstellen, die in der Regel umfassende Zugriffsmöglichkeiten auf systeminterne Daten und Funktionen besitzen.

No Security by Obscurity Obwohl sich Kerckhoffs' Prinzip ursprünglich auf kryptographische Verfahren und Algorithmen bezog, sollte es vom Grundsatz auch für alle Aspekte der Entwicklung Cybersecurity-relevanter Embedded Systeme Anwendung finden. *„Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi."* (Auguste Kerckhoffs) [8]. Frei übersetzt bedeutet Kerckhoffs' Prinzip, dass das System keiner Geheimhaltung erfordern darf, um sicher zu sein. Die Sicherheit sollte allein in der Geheimhaltung kryptographischer Geheimnisse wie Schlüssel liegen, jedoch nicht im Design oder in der Implementierung eines Systems. Dies schließt unter anderem jegliche proprietäre Verfahren zur Erfüllung von Security-Schutzzielen aus.

Bypassing und Backdoors Das Umgehen von Securityfunktionen sowie das Implementieren und Nutzen von Hintertüren ist strikt untersagt.

Literatur

1. Agentur der Europäischen Union für Cybersicherheit (ENISA). (2019). *Good practices for security of Smart cars*. https://www.enisa.europa.eu/publications/smart-cars/at_download/fullReport. Zugriffsdatum 2021-06-01.
2. Automotive Information Sharing And Analysis Center (Auto ISAC). (2016). *Best practices – Auto-ISAC*. Best Practices – Auto-ISAC. https://automotiveisac.com/best-practices/. Zugriffsdatum 2021-06-01.
3. Department for Transport. (2017). *Principles of cyber security for connected and automated vehicles*. GOV.UK. https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles. Zugriffsdatum 2021-06-01.
4. Diehl, E. (2016). *Ten laws for security*. Springer Publishing.
5. European Automobile Manufacturers Associations (ACEA). (2017). *Principles of automobile cybersecurity*. https://www.acea.auto/files/ACEA_Principles_of_Automobile_Cybersecurity.pdf. Zugriffsdatum 2021-06-01.
6. Highland, H. J. (1995). AIN'T misbehaving—A taxonomy of anti-intrusion techniques. *Computers & Security, 14*(7), 606. https://doi.org/10.1016/0167-4048(96)81669-5.

7. ISO. (2020). *ISO/SAE DIS 21434 Road vehicles – Cybersecurity engineering*.
8. Kerckhoffs, A. (1883). *La cryptographie militaire*. Published.
9. Le, V. H., et al. (2018). Security and privacy for innovative automotive applications: A survey. *Computer Communications, 132*, 17–41. https://doi.org/10.1016/j.comcom.2018.09.010
10. National Highway Traffic Safety Administration US Department of Transportation. (2016). *Cybersecurity best practices for modern vehicles*. https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/812333_cybersecurityformodernvehicles.pdf. Zugriffsdatum 2021-06-01.
11. Nilsson, D. K. & Larson, U. E. (2009). A defence-in-depth approach to securing the wireless vehicle infrastructure. *Journal of Networks*, *4*(7). https://doi.org/10.4304/jnw.4.7.552-564
12. SAE International. (2016). *J3061 – Cybersecurity guidebook for cyber-physical vehicle systems*.
13. Schnur, H. C. (1986). *Satiren (Reclams Universal-Bibliothek).* Reclam, Philipp, jun.
14. Whatley, N. (1927). Antike Schlachtfelder, Bausteine zu einer Antiken Kriegsgeschichte. Vol. IV. Part 2. J. Kromayer und G. Veith. S. 171–323. Berlin: Weidmannsche Buchhandlung, 1926. – Schlachten-Atlas zur Antiken Kriegsgeschichte, Griechische Abteilung I. Von Marathon bis Chaeronea. J. Kromayer und G. Veith. Leipzig: H. Wagner und E. Debes, 1926. *The Classical Review*, *41*(4), 147–148. https://doi.org/10.1017/s0009840x00043237.