Secure Product Lifecycle

4

Zusammenfassung

Die Umsetzung einer ganzheitlichen Cybersecurity-Strategie erfordert die Anwendung aller Vorgaben und Maßnahmen für den gesamten Lebenszyklus eines Produkts, inklusive der gesamten Liefer- bzw. Wertschöpfungskette. Die Verantwortung und der Wirkungsbereich von Cybersecurity ist nicht wie bei den meisten anderen Disziplinen auf die Entwicklungs- und Produktionsphase beschränkt, sondern überspannt sämtliche Abschnitte des Produktlebenszyklus. In der Planungsphase werden Strategie und Konzept definiert und damit Security *by Design* in der folgenden Produktentwicklung integriert. In der Entwicklungsphase wird Cybersecurity mit dem bestehenden Entwicklungsprozess verwoben und damit gleichermaßen mit den anderen Disziplinen bearbeitet. In der Produktionsphase müssen sowohl die Produktionsumgebungen des OEMs und aller Lieferanten abgesichert werden als auch die zugehörenden logistischen Prozesse. In der am längsten andauernden Lebensphase eines Produkts, der Post-Produktionsphase, müssen die Schutzmechanismen kontinuierlich an die sich verändernde Bedrohungssituation angepasst werden. Im letzten Lebensabschnitt wird dafür gesorgt, dass Geheimnisse und personenbezogene Daten vor der Außerbetriebnahme des Produkts vernichtet werden, um einen Zugriff von Dritten zu verhindern.

Der Themenkomplex Cybersecurity ist für sämtliche Abschnitte des Produktlebenszyklus relevant und überspannt somit die Planung, die Entwicklung, die Produktion, sowie auch die Phasen nach der Produktion bis zur Außerbetriebnahme, s. Abb. 4.1.

Was muss getan werden, damit in jeder Phase des Produktlebenszyklus für die Sicherheit gesorgt ist? Im Folgenden wird diese Frage für die einzelnen Abschnitte des Lebenszyklus diskutiert.

M. Wurm, *Automotive Cybersecurity,* https://doi.org/10.1007/978-3-662-64228-3_4

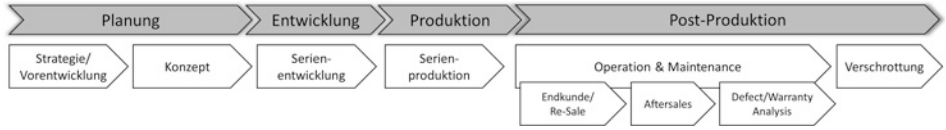

Abb. 4.1 Produktlebenszyklus

4.1 Strategie und Konzept

Der ISO-Standard 26262 [4], ist seit Jahren ein fest integrierter und stark mit der Produktentwicklung verzahnter Teilprozess der Elektronikentwicklung des Automotive-Bereichs. Wie bei der Funktionalen Sicherheit kann auch Cybersecurity nicht einfach nachträglich in ein Produkt „hineindokumentiert“ werden, sondern muss fester Bestandteil des Entwicklungsprozesses und darüber hinaus des gesamten Produktlebenszyklus sein.

Wieso ist es wichtig, dass Security von Beginn an bei der Entwicklung von Fahrzeugen und Infrastrukturkomponenten berücksichtigt wird?

Späte Änderungen an der Systemarchitektur verursachen in der Summe höhere Kosten, als wenn die Anforderungen bereits zu Beginn der Entwicklung bekannt sind. Dies ist vorwiegend den relativ langen Entwicklungszyklen sowie der Einbindung mehrgliedriger Lieferketten geschuldet.

Ein spätes Hinzufügen von Cybersecurity-Features in Elektronikkomponenten wird zur Kosten- und Zeitersparnis häufig durch ein Andocken vorgefertigter Securityfunktionen an das vorhandene System bewerkstelligt. Dabei kommt die Untersuchung potenzieller Schwachstellen des abzusichernden Systems häufig zu kurz, was zwangsläufig dazu führt, dass die Securitymaßnahmen weder vollständig noch zielgerichtet sind. Das *Security-by-Design-Prinzip* wird damit nicht erfüllt.

Eine höhere Sicherheit kann im Gegenzug dazu erreicht werden, wenn die Schwachstellen des Systems frühzeitig erkannt und analysiert werden, wenn daraus resultierende, potenzielle Risiken identifiziert und erforderliche Schutzziele formuliert werden. Die daraus abgeleiteten Securityanforderungen fließen dann idealerweise von Anfang an in die Systemarchitektur ein und werden somit regelrecht verinnerlicht, sozusagen Teil ihrer DNS. Diese Analysen sowie die daraus resultierenden Erkenntnisse dienen auch als Grundlage für die fortwährenden Securityaktivitäten im Verlauf des Produktlebenszyklus. Die Bewertung der Relevanz der vom Security-Monitoring erfassten Schwächen und Bedrohungen gelingt mittels der vorliegenden Informationen besser. Das sog. *Risk Treatment,* wird dadurch effizienter, weil die beschränkten Ressourcen für die Gegenmaßnahmen gezielt zum Reduzieren zu hoher Restrisiken verwendet werden können. Der in Abschn. 2.1 beschriebene risikobasierte Ansatz wird in diesem Teilbereich durch die in ISO 21434 definierte Methodik für die Risikobewertung realisiert.

Mit welchen konkreten Aktivitäten schafft man eine gute Basis als Ausgangslage für die Entwicklung sicherer (by-design) Produkte? Und wie sorgt man auch nach der Entwicklung, Produktion und Auslieferung an den (End-)Kunden dafür, dass die Sicherheit weiterhin gewährleistet wird?

ISO 21434 schreibt für die sog. Konzeptphase die Erstellung unterschiedlicher Arbeitsprodukte vor, die wiederum das betroffene Produkt und dessen Kontext in ausreichender Tiefe definiert. Insbesondere anhand der sog. *Item Definition* und der Identifikation möglicher Angriffsszenarien, die für die Assets des Produkts eine Bedrohung darstellen könnten, lassen sich sowohl in der Entwicklungsphase (TARA) als auch danach (Continuous Cybersecurity Activites) die Risiken von Cybersecurity-Schwächen ermitteln und angemessene Gegenmaßnahmen ableiten.

Verschiedene organisatorische Maßnahmen, s. Kap. 3, wie etwa der in UNECE WP.29 R.155 geforderten Installation eines CSMS, der Bereitstellung finanzieller und personeller Kapazitäten, sowie dem Aufbau von Security-Expertise im Unternehmen schaffen die Grundlage dafür, dass das Risiko von Cybersecurity-Angriffen gemäß standardisierter Methodik ermittelt und behandelt wird.

Nicht zuletzt ist es auch die UNECE WP.29, die für die Entwicklung von Fahrzeugen auch das Prinzip Security-by-Design zur Reduzierung von Risiken vorschreibt.

4.2 Entwicklung

Welche Maßnahmen müssen ergriffen werden, damit Security in der Produktentwicklung systematisch berücksichtigt wird?

Welche Rolle spielt der Entwicklungsprozess für die Absicherung des Produktlebenszyklus?

Hier lohnt sich ein Blick auf die bereits existierende Prozesslandschaft, insbesondere auf die Zielsetzung und Vorgehensweise der funktionalen Sicherheit (Safety). Der in der ISO-Norm 26262 spezifizierte Entwicklungsprozess für sicherheitskritische Kfz-Systeme legt für die System-, Hardware- und Softwareentwicklungsprozesse die einzelnen Methoden und Ziele fest – in ähnlicher Weise wie die zukünftige ISO-Norm 21434 dies für die Cybersecurity tut. Beide Normen verfolgen ein gemeinsames Ziel: die Entwicklung eines zuverlässigen, fehlerfreien und sicheren (safe und secure) Systems indem Risiken für Hazards und Threads möglichst reduziert werden, s. [5] und [8].

Die Integration von ISO21434-Workproducts und Methoden in ein vorhandenes Automotive-Spice-Entwicklungsmodell erfolgt ähnlich wie bei Safety, weil Safety eine vergleichbare Integration bereits abgeschlossen hat.

Einerseits bestehen Ähnlichkeiten in der Vorgehensweise und Arbeitsprodukte, s. Tab. 4.1, andererseits gibt es aber auch Unterschiede in der Sichtweise.

Tab. 4.1 Gegenüberstellung wichtiger Arbeitsprodukte von Safety und Security

	Safety	Security
Riskoanalyse	HARA (Gefährdungen/Hazards)	TARA (Bedrohungen/Threats)
Anforderungsanalyse	Safety Goals	Security Goals
Systemdesign/-architektur	Functional/Technical Safety Concept	Security Concept/Security-Architektur
Validierung	Validierung der Safety-Ziele	Security-Tests (Pentests, Fuzz-Tests, etc.)

- Die Disziplin Safety/Funktionale Sicherheit betrachtet die Wahrscheinlichkeiten für zufällige, sporadische Fehler, wie etwa Bauteilausfälle und Bitflips im Speicher, und den daraus folgenden Auswirkungen des Gesamtsystems auf seine Umwelt. Mit welcher Wahrscheinlichkeit bewirken technische Ausfälle bestimmter elektronischer Bauteile oder Komponenten ein Fehlverhalten des (elektromechanischen) Systems, was letztendlich zu einer Gefährdung von Leib und Leben der betroffenen Fahrzeuginsassen oder anderer Verkehrsteilnehmer führt?
- Die Disziplin Cybersecurity betrachtet hingegen Bedrohungen der Assets, wozu auch Safetyrisiken zählen. Bezogen auf safetyrelevante Assets werden dabei absichtlich ausgelöste Fehlerverhalten betrachtet. Angreifer (Menschen) greifen hier absichtlich und mutwillig elektronische Systeme an, wodurch wiederum direkt oder indirekt andere Menschen wie etwa Besitzer oder Verkehrsteilnehmer zu Geschädigten werden.

Ein grundsätzlicher Unterschied besteht in der jeweiligen Intention von Safety und Security: Safety dient dem Schutz des Menschen vor dem technischen System – Security dient dem Schutz des technischen Systems vor dem Menschen.

Bezogen auf den Lebenszyklus existiert ein weiterer Unterschied: Eine Safety-Risikoanalyse findet i. d. R. nur einmalig im Rahmen der Entwicklungsphase statt. Für Safety ist dies ausreichend, weil auch das bewertete System, das Produkt, spätestens am Ende der Entwicklungsphase stabil ist. Für Security stellt sich dies aufgrund einer angenommenen dynamischen Veränderung der Bedrohungslage im Verlauf des Lebenszyklus anders dar, s. *Post-Produktion.*

4.3 Produktion

Welche Maßnahmen müssen ergriffen werden, um die Manipulation von Bauteilen, Komponenten, Systemen und des Gesamtfahrzeugs sowohl innerhalb der Produktions- und Fertigungsstätten, als auch im Rahmen logistischer Aktivitäten verhindern zu können?

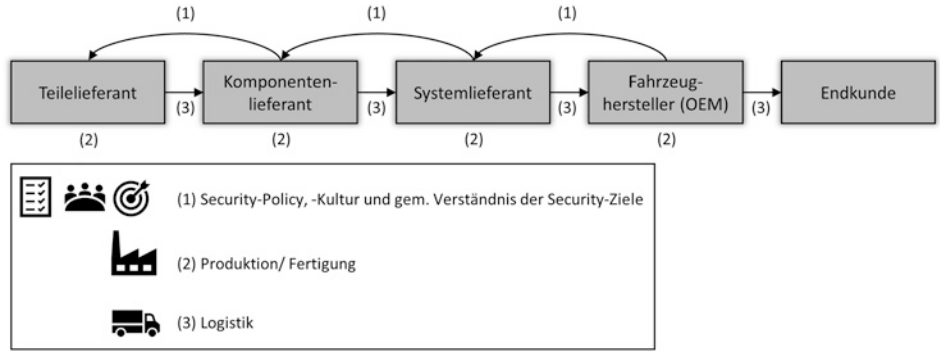

Abb. 4.2 Absicherung der Produktions- und Lieferketten

In Abb. 4.2 sind die verschiedenen Maßnahmen zum Erreichen dieser Ziele, d. h. die lückenlose Absicherung, der gesamten Wertschöpfungskette, illustriert. In der idealisierten Lieferkette – bestehend aus Teilelieferant (z. B. Halbleiterhersteller), Komponentenlieferant (z. B. ECU-Hersteller), Systemlieferant (Tier-1), OEM und Kunde – sind jeweils die Produktions- bzw. Fertigungsstätten (2) und dazwischen die Logistikprozesse (3) dargestellt. Zudem ist die Übertragung von Security-Policy, Security-Kultur und Zieldefinitionen (1) vom OEM an seine Lieferanten symbolisiert.

1. OEMs und ihre Lieferanten können die Verantwortung für bestimmte Aufgaben untereinander aufteilen – vertraglich vereinbart im sog. Development Interface Agreement. Diese Aufteilung der Verantwortung funktioniert allerdings nur dann zuverlässig, wenn unter allen Beteiligten, d. h. OEMs und Lieferanten, ein gemeinsames Verständnis für die Security-Ziele, -Meilensteine und -Anforderungen vorherrscht. Der OEM trägt für ein gemeinsames Verständnis bei, indem er u. a. die Werte seiner Security-Kultur und die Vorgaben seiner *Security-Policies* an seine Lieferanten überträgt bzw. auf sie ausdehnt, s. Kap. 3.
   Die Umsetzung der Security-Policies, die korrekte und vollständige Integration eines Security-Entwicklungsprozesses oder auch die Umsetzung geeigneter Absicherungsmaßnahmen für Logistik und Produktion können vom OEM mittels Assessments, Prozess-Audits und Begehungen der Produktionsstätten kontrolliert werden.
2. Die Absicherung der jew. *Produktionsumgebung* jedes einzelnen beteiligten Unternehmens in der Lieferkette wird im Abschn. 5.5.3 näher ausgeführt.
3. Absicherung der *Logistik* zwischen den jew. Unternehmen bzw. Produktionsstätten: Dabei muss insbesondere der nicht autorisierte Zugriff auf die Komponenten kontrolliert bzw. verhindert werden. ISO 21434 sieht zur Definition produktionsspezifischer Securityanforderungen und Schutzmaßnahmen den sog. *Production Control Plan* vor (Clause 12).

4.4 Post-Production

Wieso spielt Security auch nach der Entwicklung und der Produktion noch eine wichtige Rolle?

Die Bedrohungslage bzgl. Cyberangriffe auf Fahrzeuge verändert sich fortlaufend. Einerseits werden Schwächen im System, die zum Zeitpunkt der Entwicklung noch unbekannt waren, im Laufe der Zeit beispielsweise durch Security-Forschungsaktivitäten bekannt. Aufgrund der komplexen und umfangreichen Funktionalität in Fahrzeugsystemen ist es dabei keine Frage, ob eine Security-Schwachstelle vorhanden ist und entdeckt wird, sondern nur wann sie bekannt wird. Anhand eines Event-Assessments werden neu erkannte Schwächen und Bedrohungen jeweils hinsichtlich ihrer möglichen Auswirkungen und hervorrufenden Risiken bewertet. Darauf basierend wird letztendlich auch entschieden, ob eine Behebung der Schwachstelle nötig ist, bzw. wie die Kritikalität der Schwachstelle einzustufen ist. Andererseits verändern sich mit der Zeit auch die Annahmen, die für die Gestaltung des Angreifermodells herangezogen wurden. So muss etwa von stetig wachsenden Fähigkeiten und Kenntnissen der Angreifer, sowie verbesserten Werkzeugen ausgegangen werden. Angreifer entwickeln stets neue Methoden, um Angriffe auf Fahrzeuge und Infrastruktur erfolgreich durchzuführen. Die verfügbare Rechenleistung zum Durchführen kryptoanalytischer Berechnungen, d. h. zum Brechen kryptographischer Verfahren, kann heutzutage fast beliebig erweitert werden, etwa durch sog. Crowd-Computing. Selbst die aktuell gültige Annahme, dass Quantencomputer noch nicht mit ausreichender Anzahl sogenannter Qubits verfügbar sind könnte bereits in wenigen Jahren überholt sein, s. *Hintergrundinformationen zu Post-Quantum Computing.*

Hintergrund

Post-Quantum Computing

Was sind Quantencomputer?

Quantencomputer sind fortgeschrittene Rechnersysteme, die für ihre Berechnungen bestimmte Phänomene der Quantenmechanik ausnutzen – etwa die sog. Quantenverschränkung (engl. entanglement), die Albert Einstein angeblich noch als „spukhafte Fernwirkung“ bezeichnete. Verschränkte Quantenobjekte verhalten sich hinsichtlich ihres Zustands als Einheit, auch über große Distanzen hinweg und ohne Zeitverzögerung. Die Realisierung von Quantencomputern mit ausreichender Anzahl von *Qubits,* den sog. Quantenbits als Äquivalent klassischer Bits, steht noch aus, aber in der Theorie kann ein Quantencomputer aufgrund seiner Rechengeschwindigkeit schwierige Probleme effizient und in endlicher Zeit lösen, wozu klassische Computer nicht fähig sind.

Die Technologie der Quantencomputer wird für einige Anwendungen nutzbringend sein. So nutzt die sog. *Quantenkryptographie* bestimmte quantenmechanische

Effekte, um kryptographische Verfahren und Algorithmen schneller bzw. sicherer umzusetzen als mit herkömmlichen Rechnersystemen.

Ein erstes Beispiel ist der *Quantenschlüsselaustausch.* Das Schlüsselmaterial wird hierbei mittels Photonen über eine optische Verbindung, etwa Glasfaserleitungen, übermittelt. Die Abhörsicherheit kommt dadurch zustande, dass das Abhören, bzw. Messen der Informationen, etwa der Polarisationszustand der einzelnen Photonen, deren Zustand ändert. Die ursprüngliche Information wird zerstört und das Abhören würde dadurch erkannt werden. Aufgrund der geringen Bandbreite und Reichweite ist dieses Verfahren nur eingeschränkt praxistauglich.

Ein weiteres Beispiel ist die Erzeugung von Zufallszahlen. Mittels quantenmechanischer Effekte können echte, unvorhersagbare Zufallswerte generiert werden. Machine Learning-Algorithmen und zahlreiche Optimierungsaufgaben sind weitere Anwendungsgebiete, die von den Fähigkeiten eines Quantencomputers profitieren werden.

Wieso werden Quantencomputer zur Bedrohung für die heutige Kryptographie?

Die Sicherheit der heute verwendeten kryptographischen Algorithmen beruht auf der Annahme, dass (noch) kein effizientes Verfahren existiert, bzw. kein Rechnersystem schnell genug ist, die dafür erforderlichen kryptoanalytischen Berechnungen in endlicher Zeit auszuführen. Der Rechenaufwand für die Kryptoanalyse, d. h. für das Brechen eines Kryptosystems, steigt exponentiell mit der Schlüssellänge und wird somit mit einem hinreichend langen Schlüssel praktisch nicht machbar.

Das sog. Faktorisierungsproblem für ganze Zahlen beschreibt das Fehlen eines effizienten Verfahrens, mit dem etwa beim RSA-Kryptosystem der Modulus faktorisiert werden könnte, um das Kryptosystem zu brechen.

Für den sog. diskreten Logarithmus, der u. a. die Grundlage für das ElGamal-Verfahren und ECDSA bildet, verhält es sich ähnlich. Mit Algorithmen wie etwa der *Babystep-Giantstep-Methode* kann der diskrete Logarithmus zwar schneller berechnet werden als durch wahlloses Durchtesten. Es ist allerdings auch hier kein effizienter Algorithmus bekannt, dessen Rechenaufwand durch lineares Erhöhen der Schlüssellänge keine exponentielle Steigerung erfährt.

Die Sicherheit symmetrischer Verfahren wie AES beruht auf der schieren Größe des Schlüsselraums. Bei einem 128 Bit langen Schlüssel benötigt ein moderner Supercomputer etwa 10 Billiarden Jahre für einen Brute-Force-Angriff.[1]

[1] Diese Rechnung basiert auf der Leistungsfähigkeit moderner Supercomputer, die in der Größenordnung von etwa 100 PFLOPS liegt, und auf der Annahme, dass rund 100 Rechenoperationen pro Entschlüsselungsversuch benötigt werden. 100 PFLOPS/100 Operationen pro Entschlüsselungsversuch $= 10^{15}$ Entschlüsselungsversuche pro Sekunde $= 3{,}1 * 10^{22} =$ Entschlüsselungsversuche pro Jahr. Bei einer Schlüssellänge von 128 Bit sind zum vollständigen Durchprobieren 2^{128} Versuche erforderlich. $3,4 * 10^{38} Versuche / 3,1 * 10^{22} VersucheproJahr = 10^{16} Jahre$

Im Gegensatz zu heutigen Rechnersystemen existieren für Quantencomputer bereits seit vielen Jahren Algorithmen, die die oben beschriebenen Probleme effizient berechnen können und damit die Analyse heutiger Kryptosysteme ermöglichen.

- Der *Shor-Algorithmus* [7] kann mithilfe eines Quantencomputers die Integerfaktorisierung sowie den diskreten Logarithmus in polynomieller Laufzeit durchführen, d. h. der Rechenaufwand steigt nur linear mit der Schlüssellänge. Somit kann ein Quantencomputer mit genügender Rechenleistung dieses Problem in kurzer, endlicher Zeit lösen.
- Der *Grover-Algorithmus* [3] ermöglicht bei symmetrischen Verfahren und Hashverfahren ein schnelleres Durchprobieren aller möglicher Kombinationen (Brute-force). So wird etwa bei einer AES 128-Verschlüsselung die maximale Anzahl benötigter Versuche von 2^{128} auf 2^{64} verkürzt, was einer Halbierung der Schlüssellänge gleichkommt.

Die Folgen auf den Embedded-/Automotive-Bereich werden verheerend sein. Die zur Absicherung der verschiedenen Security-Bausteine verwendeten kryptographischen Algorithmen wie etwa RSA- und ECC-basierte Verschlüsselungs- und Signaturverfahren, werden von Quantencomputern nachhaltig kompromittiert werden können. Auch Hash-Verfahren und symmetrische Kryptosysteme mit zu kurzen Schlüsseln werden betroffen sein. Daraus folgt, dass die meisten der heute eingesetzten kryptographischen Verfahren als unsicher einzustufen sind, sobald Quantencomputer mit ausreichender Performanz verfügbar sein werden.

Ist das ein Grund zur Sorge? Es gibt doch noch gar keine Quantencomputer!
Quantencomputer werden voraussichtlich bald Realität sein. Diese Aussage teilen sich verschiedene Forscher und Experten aus den Bereichen Kryptologie und Informatik und sie nennen Zeiträume zwischen 10 bis 20 Jahre bis die ersten Quantencomputer mit genügend Rechenleistung verfügbar sein werden.

Die Antwort auf die einleitende Frage ist also: Nein, aktuell besteht kein akuter Grund, sich Sorgen zu machen. Zumindest noch nicht. Aber ein baldiges Handeln ist erforderlich.

Der zeitliche Vorsprung wird hier zum kritischen Faktor. Auf der einen Seite wird genügend Zeit benötigt, um gegen Post-Quantum-Computing sichere Algorithmen (PQC-Algorithmen) zu finden, auszuwählen, zu implementieren und in die Systeme zu integrieren. Auf der anderen Seite erschweren die langen Fahrzeug-Entwicklungszyklen und die lange Produktlebensdauer ein kurzfristiges und flexibles Handeln.

Beispielrechnung: Bei einer etwa 5 Jahre dauernden Entwicklung und einer anschließenden 5 Jahre dauernden Serienproduktion sowie einer geschätzten Nutzungsdauer beim Endkunden von 10 bis 15 Jahren reichen die heute getroffenen Entwicklungsentscheidungen mindestens 20 Jahre in die Zukunft. Falls Quantencomputer in 20 Jahren verfügbar sein sollten, sind bereits die heute entwickelten

Fahrzeuge davon gefährdet. Software und Daten, die mit den heute üblichen kryptographischen Verfahren verschlüsselt oder digital signiert werden, können in Zukunft von Quantencomputern wieder entschlüsselt bzw. kompromittiert werden.

Welche Vorkehrungen müssen getroffen werden und welche Auswirkungen hat dies auf Automotive Systeme (ECUs)?
Hashfunktionen und symmetrische Verfahren der „klassischen" Kryptographie können von Quantencomputern nicht vollständig gebrochen werden. Quantencomputer können lediglich die *Exhaustive-Search-Methode* (Brute force) beschleunigen. Um das heutige („Prä-Quantum-Computing") Sicherheitsniveau zu erhalten, ist demnach eine Vergrößerung (mindestens Verdoppelung) der Hashlänge bzw. der Schlüssellänge für symmetrische Verfahren ausreichend.

Dies wirkt sich sowohl auf den erforderlichen statischen und dynamischen Speicherbedarf als auch auf den Rechenaufwand für die kryptographischen Algorithmen aus.

Als Ersatz für die von Quantencomputern gefährdeten, asymmetrischen Algorithmen existieren bereits zahlreiche verschiedene PQC-Kryptoalgorithmen. Weitere befinden sich in der Entwicklungs- oder Evaluationsphase.

PQC-Kryptoalgorithmen sind auf klassischen Rechnersystemen lauffähig, sind aber dennoch gegen die oben aufgeführten, kryptoanalytischen Angriffe durch Quantencomputern geschützt. Sie können anhand der mathematischen Probleme, auf denen sie basieren, klassifiziert werden, vgl. [2]:

- multivariate Polynomgleichungen
- mathematische Gitter
- Isogenie elliptischer Kurven
- kryptographische Hashfunktionen
- fehlerkorrigierende Codes

Post-Quantum-Computing ist seit einigen Jahren Gegenstand verschiedener Forschungsprojekte und Standardisierungsaktivitäten.

In *PQCrypto,* einem EU-Projekt des Horizon 2020-Programms [6], wurde eine mögliche Post-Quantum-Kryptographie für die Internet-Kommunikation, das Cloud-Computing und für Low-Power-Devices untersucht. Letzteres Arbeitspaket könnte auch für Anwendungen im Automotive-/Embedded-Bereich interessant sein.

PROMETHEUS, ebenfalls ein EU-Projekt des Horizon 2020-Programms, zielt auf PQ-Signatur- und Verschlüsselungsverfahren ab, die auf mathematische Gitter basieren.

Darüber hinaus existieren viele weitere Forschungsaktivitäten, auch außerhalb der EU.

Bei den Standardisierungsaktivitäten ist neben ISO, IETF und ETSI der von NIST ausgerufene Wettbewerb, s. [1], für die Evaluierung und Auswahl geeigneter PQC-Algorithmen für Verschlüsselungsverfahren, Signaturverfahren und Schlüsselaustauschverfahren eine wichtige Referenz.

Neben der Standardisierung und Auswahl geeigneter PQC-Algorithmen wird zukünftig auch die sog. *Krypto-Agilität* für die langlebigen Automotive-Systeme eine große Rolle spielen. Systeme mit entsprechender Update-Fähigkeit – bestenfalls auch für Krypto-Beschleuniger – erlauben ein Upgrade und Austauschen kryptographischer Algorithmen, ohne die Hardware austauschen zu müssen.

Welche Eigenschaften sollten PQC-HSMs zukünftig besitzen? Wang und Stöttinger gingen dieser Frage nach, s. [11]. Sie trafen eine Auswahl von insgesamt vier PQC-Verfahren, die für Anwendungen im Automotive-Umfeld taugen und (unter-)suchten die HSM-Architektur, die diese PQC-Algorithmen hinsichtlich Laufzeit- und Speicheranforderungen am besten unterstützen, etwa Hardwarebeschleuniger für PQC-Algorithmen wie SHA3-512 und AES256.

Handlungsempfehlungen:
Aufgrund der langen Laufzeiten, s. oben, sollten bereits heute Vorbereitungen getroffen werden, um auf mögliche, zukünftige Bedrohungen durch Quantencomputer reagieren zu können.

- Die securityrelevante Hardware (z. B. HSM) sollte möglichst Update-fähig sein und über ausreichende Reserven hinsichtlich CPU-Laufzeit und Speicher verfügen, um zu einem späteren Zeitpunkt mit geeigneten PQC-Algorithmen ausgestattet werden zu können.
- Verschiedene Migrationsszenarien für den möglichen Umstieg auf die Post-Quantum-Kryptographie sollten geplant werden – ggf. kann übergangsweise auch zweigleisig gefahren werden, d. h. die bisherigen Verfahren der klassischen Kryptographie und PQC-Algorithmen als Backup bzw. zur Evaluation werden gleichzeitig verwendet.
- Entwicklungsentscheidungen sollten vorausschauend getroffen werden, insbesondere wenn es sich um PKI-Infrastruktur, Hardware-Design und der Planung von Reserven handelt. Besonders kritische Entscheidungen, etwa bzgl. Telematik-/Connectivity-ECUs und Gateway-ECUs, sollten ggf. vorgezogen und frühzeitig getroffen werden.
- Die Forschungs- und Standardisierungsaktivitäten sollten in den kommenden Jahren sorgfältig verfolgt werden und die eigenen Migrationspläne ggf. nachjustiert werden. ◀

Welche Algorithmen sind unsicher, mittelfristig sicher oder sogar langfristig sicher? Die entsprechenden Einschätzungen von BSI oder auch NIST bzgl. der Verwendung kryptographischer Verfahren ist ebenfalls nicht stabil, sondern verändert sich im Laufe der

Zeit aufgrund neuer Erkenntnisse, etwa falls in einem kryptographischen Verfahren eine Hintertür entdeckt wurde, die etwa von einem Geheimdienst hineinspezifiziert wurde.

Das Angreifermodell muss spätestens dann angepasst werden, falls etwa eine neue, bisher nicht betrachtete Angreiferklasse für das jeweilige Produkt relevant wird. UNECE R.155 fordert darüber hinaus eine jährliche Aktualisierung der TARA durch den OEM – für die komplette Produktlebensdauer. Beispiel: Eine neu formierte, weltweit agierende Aktivistengruppe mit großen finanziellen Ressourcen, die die Einführung autonom fahrender Fahrzeuge um jeden Preis und mit allen Mitteln verhindern wollen, greifen gezielt diese Fahrzeuge und deren Hersteller an und erpressen sie.

Zusammenfassung
Die veränderliche Bedrohungslage, s. oben, kann sich auch für Fahrzeuge, die sich bereits im Einsatz beim Kunden befinden, negativ auswirken. Verglichen mit der Ausgangslage zum Zeitpunkt der Entwicklung könnte die neue, veränderte Situation zu einem erhöhten, nicht akzeptablen Risiko für den Kunden führen. Die Auswirkungen könnten von kleinen Funktionseinschränkungen bis zu safetykritischen Funktionsstörungen reichen. Letzteres müsste vom OEM so schnell wie möglich korrigiert und behoben werden, weil der OEM in der Verantwortung ist, die Sicherheit seiner Produkte auch nach der Auslieferung an den Kunden sicherzustellen, s. [9] und [10].

Anforderungen
Cybersecurity begleitet das Fahrzeug über seinen gesamten Lebenszyklus hinweg. Die Annahmen, die in der Design- und Entwicklungsphase etwa für die TARA zum Angreifermodell und zu den operativen Bedingungen getroffen wurden, müssen aufgrund der Unbeständigkeit der Bedrohungslage über den gesamten Lebenszyklus regelmäßig überprüft und infrage gestellt werden. Falls ein derartiges Re-Assessment das Potenzial neuer Risiken anzeigt, so müssen diese bewertet und ggf. durch geeignete Maßnahmen behoben werden. ISO 21434 definiert als sog. *Continuous Cybersecurity Activities,* die vor allem nach der Produktion relevant sind, folgende Aktivitäten: Cybersecurity Monitoring, Event Assessment und Vulnerability Management.

- Das *Cybersecurity-Monitoring* dient als zusätzliche, interne Informationsquelle, um eventuelle Angriffe bzw. Angriffsversuche auf einzelne Fahrzeuge oder die Fahrzeugflotte eines OEMs zu erkennen, s. Abb. 4.3. Die technische Umsetzung erfolgt beispielsweise mit Hilfe eines Intrusion Detection Systems, das im Fahrzeug Anomalien oder Angriffsversuche erkennt und an das zentrale Monitoringsystem im Backend, dem SOC, zur Auswertung übermittelt.
- Im Rahmen des anschließenden *Event Assessments* werden die vorliegenden Informationen u. a. anhand einer Schwachstellenanalyse untersucht. Ziel ist es hierbei festzustellen, ob sich die gefundenen Schwachstellen etwa über einen noch unbekannte Angriffspfade als kritische Probleme herausstellen, genauer gesagt ein sog. *Damage Szenario* auslösen könnten.

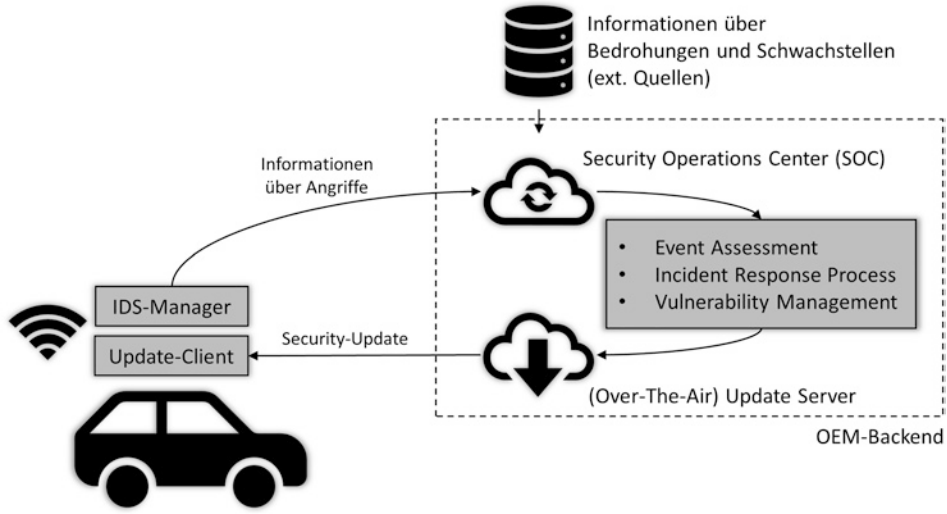

Abb. 4.3 Security-Aktivitäten in der Post-Production-Phase

- Das *Vulnerability Management* legt anhand der sog. Treatment Decision fest, ob und wie die kritischen Schwachstellen behoben werden. Das zukünftig von der UNECE WP.29 vorgeschriebene Software Update Management System (SUMS) soll unter anderem exakt für diesen Anwendungsfall die Möglichkeit schaffen, Security-Patches auf betroffene Fahrzeuge auszurollen, um kritische Schwachstellen zeitnah und kostengünstig (verglichen mit Rückrufaktionen) umzusetzen.

Die *Post-Production-Phase,* s. oben, deckt mehrere Anwendungsfälle ab – dargestellt durch verschiedene Teilphasen: Der normale Einsatz beim Endkunden, wofür das Fahrzeug vorbestimmt ist (engl. Operations), Wartungsarbeiten und Kundendienst (engl. Service and Maintenance), Aftermarket-Anwendungen, sowie Fehler- und Gewährleistungsanalysen. Letzterer Anwendungsfall führt aufgrund seiner oftmals irreversiblen Methoden zur anschließenden Außerbetriebnahme und Verschrottung. Prinzipiell gelten die oben definierten Anforderungen für alle Teilphasen.

4.5 Außerbetriebnahme und Verschrottung

In der allerletzten Phase des Produktlebenszyklus, der *Außerbetriebnahme* (engl. decommissioning), dürfen elektronische Komponenten, die sensible Informationen beinhalten, nicht einfach dem Materialsammlungs- und entsorgungsprozess zugeführt werden. Problematisch sind in diesem Zusammengang alle sensiblen und z. T. auch kritischen Daten, wie etwa personenbezogene Daten, kryptographisches Material und

Firmengeheimnisse (Intellectual Property). Diese Daten müssen zuvor mit sicheren Methoden gelöscht bzw. unbrauchbar gemacht werden, ansonsten könnten Angreifer durch Zugriff auf die Materialströme der Entsorgungs- und Recyclingprozesse intakte, wiederverwendbare Informationen erhalten und für zukünftige Angriffe ausnutzen, s. Abschn. 5.1.6.

Literatur

1. Alagic, G., et al. (2020). *Status report on the second round of the NIST post-quantum cryptography Standardization Process.* NIST – US Department of Commerce.
2. Campos, F. (2019). Post-quantum cryptography for ECU security use cases. In M. Meyer, S. Sanwald, M. Stöttinger, & Y. Wang (Hrsg.), *17th escar Europe: Embedded security in cars* (S. 155–169). Ruhr-Universität Bochum.
3. Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96. Published. https://doi.org/10.1145/237814.237866.
4. ISO. (2011). ISO 26262 – *Road vehicles – Functional safety, Part 1–10. ISO/TC 22/SC 32 – Electrical and electronic components and general system aspects.*
5. Macher, G., et al. (2020). *An Integrated View on Automotive SPICE*. SAE Technical Paper Series. Published. https://doi.org/10.4271/2020-01-0145.
6. Post-quantum cryptography for long-term security PQCRYPTO. (2015). PQCRYPTO. https://pqcrypto.eu.org/. Zugriffsdatum 2021-06-01.
7. Shor, P. W. (1997). Polynomial-Time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing, 26*(5), 1484–1509. https://doi.org/10.1137/s0097539795293172.
8. Skoglund, M., et al. (2018). In search of synergies in a multi-concern development lifecycle: Safety and cybersecurity. *Developments in Language Theory, 302–313*. https://doi.org/10.1007/978-3-319-99229-7_26.
9. UN Regulation No. 155 - Cyber security and cyber security management system | UNECE. (2021, 4. März). UNECE.ORG. 2021-06-01.https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security. Zugriffsdatum 2021-06-01.
10. UN Regulation No. 156 – Software update and software update management system | UNECE. (2021, 4. März). UNECE.ORG. https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update. Zugriffsdatum 2021-06-01.
11. Wang, W., & Stöttinger, M. (2020). *Post-Quantum secure architectures for automotive hardware secure modules*. Published.