Security-Organisation und -Management

3

Zusammenfassung

Wie kann Cybersecurity nachhaltig und effizient eingeführt, überwacht und gesteuert werden? Wie kann Cybersecurity systematisch mit den übergeordneten Zielen eines Unternehmens verknüpft und in Einklang gebracht werden? Vor welchen Aufgaben stehen dabei die Abteilungsleiter und die Unternehmensführung? Die sog. *Cybersecurity-Governance* muss in der Unternehmensführung verankert sein. Eine lebendige Cybersecurity-Kultur, die in der gesamten Belegschaft nachhaltig für ein besseres Bewusstsein für Cybersecurity sorgt, ist für alle Seiten ein Gewinn. Zu den weiteren Aufgaben zählen Planung und Durchführung von Audits und Zertifizierungen, sowie das Etablieren fortlaufender Cybersecurity-Aktivitäten, insbesondere für das Event Monitoring und Incident Response Management.

In diesem Kapitel wird ausgeführt, wieso nicht nur die technischen Maßnahmen zur Absicherung der Fahrzeuge und deren Komponenten erforderlich sind, sondern wieso auch die Verwaltung aller Cybersecurity-Aktivitäten in der gesamten Wertschöpfungskette und über den gesamten Produktlebenszyklus hinweg eine wichtige Voraussetzung für den ganzheitlichen Schutz darstellt.

© Der/die Autor(en), exklusiv lizenziert durch Springer-Verlag GmbH, DE, ein Teil von Springer Nature 2022

M. Wurm, *Automotive Cybersecurity,* https://doi.org/10.1007/978-3-662-64228-3_3

3.1 Welche organisatorischen Maßnahmen sind erforderlich?

Wieso sind organisatorische Maßnahmen für den Schutz vor Cyberangriffen erforderlich? Sind technische Maßnahmen zur Absicherung nicht ausreichend?
Wie kann Cybersecurity nachhaltig und effizient eingeführt, überwacht und gesteuert werden? Wie kann Cybersecurity systematisch mit den übergeordneten Zielen eines Unternehmens verknüpft und in Einklang gebracht werden? Vor welchen Aufgaben stehen dabei die Abteilungsleiter und die Unternehmensführung?

Mit der Einführung eines sog. *Cybersecurity Management Systems* (CSMS) werden in Analogie zu einem *Information Security Management System* (ISMS) Abläufe und Regeln aufgestellt, die innerhalb einer Organisation nachhaltig und systematisch alle Cybersecurity-Aktivitäten beschreiben, einführen, überwachen, steuern und fortlaufend nachjustieren und verbessern.

Das „Weltforum für die Harmonisierung der Fahrzeugvorschriften“ (WP.29) der UNECE (United Nations Economic Commission for Europe) hatte im Jahr 2020 für die aktuell rund 60 UNECE-Mitgliedsländer zwei neue Vorschriften zur Gewährleistung der Fahrzeugsicherheit und explizit auch zum Schutz gegen Cyberangriffe, verabschiedet.

Die von der UNECE WP.29 herausgegebenen Verordnungen R.155 [1] und R.156 [2] sind dabei einerseits ein Versuch, die multiperspektifischen Fragen und Problemstellungen für die Automobilindustrie zu beantworten und andererseits, um einen rechtlichen Rahmen für die Entwicklung von nachhaltig sicheren Fahrzeugen zu schaffen. Mit diesen beiden Vorschriften werden auch zum ersten Mal Maßnahmen zum Schutz von vernetzten und autonomen Fahrzeugen angeordnet. Sie bestehen aus vier Arbeitspaketen:

- *Management* von fahrzeugrelevanten Risiken durch Cyberangriffe
- Anwendung des *Security by Design*-Prinzips über die gesamte Wertschöpfungskette hinweg
- Erkennen von *Security-Vorfällen* innerhalb der gesamten Fahrzeugflotte sowie Veranlassen von geeigneten Reaktionen
- Einführung einer rechtlichen Grundlage von *Over-the-Air-Updates* für die Fahrzeugsoftware, basierend auf einer sicheren (safe und secure) Software-Updatefunktion

Das in UNECE WP.29 R.156 geforderte *Software Update Management System* (SUMS) wird im Abschnitt *Sicheres Update,* s. Abschn. 5.5.4, erneut aufgegriffen und erläutert.

Im nächsten Abschnitt wird das in UNECE WP.29 R.155 geforderte Cybersecurity Management System (CSMS) diskutiert.

3.2 Welche Anforderungen werden an das Security-Management gestellt?

Als Grundlage für die Umsetzung eines CSMS sowie für dessen Zertifizierung, die von UNECE WP.29 zukünftig für die Typenzulassung erforderlich ist, dient der Cybersecurity Engineering Standard ISO 21434. In diesem Abschnitt werden Bestandteile, die für die Security-Organisation und Management relevant sind, herausgegriffen und erörtert.

Cybersecurity-Governance
Wie wird sichergestellt, dass Cybersecurity keine „Eintagsfliege" ist und nach Abschluss eines Entwicklungsprojekts wieder eingestellt wird, sondern dass Cybersecurity langfristig und nachhaltig zu einem festen Bestandteil der Unternehmensstrategie wird?

Die Gefahr besteht, dass ohne Rückendeckung des Top-Managements und Verankerung in den Strategiepapieren des Unternehmens die Ressourcen, die für die Bearbeitung und Verfolgung von Cybersecurity-Aktivitäten erforderlich sind, mehr oder weniger kurzfristig wieder abgezogen werden. Zuallererst ist ein Commitment des Vorstands erforderlich, das Cybersecurity, d. h. die Absicherung der Produkte vor Cyberangriffen, als ein zu verfolgendes Unternehmensziel identifiziert und als solches durch alle Ebenen der Unternehmenshierarchie nach unten auf die Arbeitsebene ableitet.

Durch Cybersecurity, genauer gesagt durch die Nicht-Bearbeitung von Cybersecurity, können Risiken entstehen, die nicht zuletzt auch vom Management als unternehmerische Risiken verstanden werden müssen. Auf der Grundlage dieser Entscheidungen nimmt das Unternehmen die entsprechenden Vorgaben in seine Richtlinien auf und leitet davon wiederum Prozesse, Handlungsanweisungen und Rollenbeschreibungen ab. Dabei ist von Anfang an zu beachten, dass das Erzielen einer ganzheitlichen Cybersecurity-Strategie auch impliziert, dass alle Vorgaben und Maßnahmen für den gesamten Lebenszyklus eines Produkts, s. Kap. 4, sowie für die gesamte Lieferkette bzw. Wertschöpfungskette anzuwenden sind. Dies hat konkret zur Folge, dass die Einhaltung der Cybersecurity-Policies auch beim Lieferantenmanagement einfließen und von den Lieferanten eingefordert werden muss. Die Herausforderung besteht hierbei in der Definition und Einigung auf einen gemeinsamen Nenner – eine minimale Security-Strategie, die für die gesamte Zuliefererkette durchgängig gültig und anwendbar ist.

Eine weitere Aufgabe der Leitungsebene besteht im Bereitstellen ausreichender Ressourcen für das Bearbeiten der Cybersecurity-Aktivitäten. Die Kosten für Personal, Werkzeuge, Bauteile, Entwicklungs- und Testkapazitäten, etc. müssen rechtzeitig und langfristig geplant, budgetiert und durchgesetzt werden. Die Langfristigkeit führt in diesem Zusammenhang zu einer neuen Erschwernis für die Autobauer. Denn die UNECE-Anforderungen verpflichten die OEMs, dafür Sorge zu tragen, dass ihre Fahrzeuge auch nach SOP, in der sogenannten Post-Produktionsphase, sicher sein sollen, indem Schwachstellen erkannt und behoben werden. Die wirtschaftliche Abschätzung

dieser Anforderung und der damit verbundenen, langfristigen Auswirkungen auf das Unternehmen sind herausfordernd. Was die Zukunft bringen wird ist ungewiss. Aber ein Blick in die jüngste Vergangenheit, fünf bis zehn Jahre sind dabei völlig ausreichend, lassen erahnen, auf welche technischen und organisatorischen Herausforderungen sich OEMs und Zulieferer einstellen sollten. Zehn Jahre nach Entwicklungsabschluss noch Bugfixes für ein dann altes System zu erzeugen, zu testen und auszurollen ist technisch und organisatorisch schwierig. Die erforderliche Entwicklungs- und Testumgebungen über so einen langen Zeitraum zu erhalten bzw. im Bedarfsfall wiederherzustellen ist aufwendig und nicht trivial. Hinzu kommt, dass ab einem gewissen Punkt die technischen Grenzen der Software-Updatebarkeit erreicht sein werden und stattdessen alternative Lösungen wie etwa das Austauschen der Hardware-Plattform erwogen werden müssen.

Eine häufige Maßnahme, um zumindest längerfristig die Wirksamkeit von Security-Aktivitäten messen und vergleichen zu können, ist die Einführung von Metriken und die regelmäßige Erhebung entsprechender Daten. Nach einem Abgleich mit den Daten des Incident-/Event Monitorings bzw. der Schwachstellenanalyse können etwas belastbarere Nachweise für Wirksamkeit und Kosten erbracht werden. Welche Kosten entstehen durch das Beheben von Security-Schwächen in aktuellen/älteren Produkten? Konnten erfolgreiche Angriffe aufgrund fehlender Security-Maßnahmen durchgeführt werden?

Erschwerend kommt hinzu, dass sich Security als Verkaufsargument bislang nicht durchsetzen konnte. Security-Maßnahmen erhöhen zwar die Qualität eines Produkts, aber nur zu geringen Teilen den Funktionsumfang. Spätestens seit der Einführung der DSGVO steigt bei den Endkunden das Bewusstsein für Datenschutz und seit der öffentlichkeitswirksamen Darstellung erfolgreicher Hackerangriffe auf verschiedene Automobilhersteller darüber hinaus auch für Security. So besteht Hoffnung, dass zukünftig ein überzeugendes Securitykonzept durchaus auch als *Selling-Point* nachgefragt werden wird.

Verknüpft mit dem Aufbau von Ressourcen ist auch die Stellenbesetzung sowie das Einsetzen von Security-Teams mit breit ausgebildeten und erfahrenen Security-Spezialisten, -Architekten, -Testern, und -Entwicklern und Teamleitern, die sich exklusiv der Bearbeitung der securitybezogenen Aufgaben widmen können.

Wie wird Cybersecurity in die existierenden Unternehmensabläufe integriert und wie wird der notwendige Informationsaustausch abgestimmt? Diese organisatorische Herausforderung besteht darin, den Austausch zwischen den verschiedenen Teams, inklusive des Security-Teams, zu fördern. Cybersecurity ist ein Querschnittsthema, welches ähnlich wie *Funktionale Sicherheit* mit quasi allen anderen Disziplinen verknüpft ist. Ein Arbeiten in „Silos“ sollte (auch) deshalb systematisch verhindert werden.

Cybersecurity-Kultur

Unter Cybersecurity-Kultur versteht man das angemessene Verhalten aller Mitarbeiter im Umgang mit Cybersecurity, das wiederum einhergeht mit der (inneren) Zustimmung zu den Werten, für die Cybersecurity einsteht. Während der Begriff Cybersecurity-Kultur

eher die innere Haltung gegenüber Cybersecurity beschreibt, sozusagen ein Bauchgefühl ist, versteht man unter *Cybersecurity-Awareness* das Bewusstsein und Wissen um die Ziele von Cybersecurity und um die Gefahren von Cybersecurity-Bedrohungen. Letzteres ist demnach eher eine Kopfsache.

Die Cybersecurity-Kultur sollte zu einem Teil der Unternehmenskultur werden und zu einem festen Bestandteil in der täglichen Arbeit eines jeden Mitarbeiters – vom Toplevel-Management bis zum Angestellten. Sicherlich hat ein Security-Ingenieur in seinem Tagesgeschäft naturgemäß mehr Berührungspunkte mit diesem Themenbereich als beispielsweise ein Lagerarbeiter. Aber auch letzterer kann durch leichtfertiges Handeln bzw. durch Vernachlässigen bestimmter Schutzbestimmungen die Sicherheit des Unternehmens gefährden.

Das oben erwähnte Verhalten jedes einzelnen Mitarbeiters ist die Grundlage für eine nachhaltige Cybersecurity-Kultur. Es sollte positiv verstärkt, gefördert aber auch trainiert werden. Hier kommt wieder die Awareness ins Spiel, d. h. im Rahmen des Security-Managements sollten Richtlinien verfasst und ein Budget bereitgestellt werden, um die Mitarbeiter aller Ebenen regelmäßig hinsichtlich ihrer Cybersecurity-Kompetenzen weiterzubilden. Dies sollte explizit sowohl die möglichen Gefahren, die von Schwachstellen ausgehen, als auch die resultierenden Risiken für das Unternehmen und seine Kunden beinhalten. Im nächsten Schritt kann dieses Programm zum Fördern und Aufrechterhalten der Awareness auf die Zulieferkette erweitert werden. Auf diesem Weg soll ein Bewusstsein und Verständnis für die Notwendigkeit und den Nutzen von Cybersecurity im gesamten Unternehmen entstehen und sich weiterentwickeln. Die Unterstützung aller Managementebenen ist dabei eine Voraussetzung für die Nachhaltigkeit der getroffenen Maßnahmen. Darüber hinaus setzt die Nachhaltigkeit einen kontinuierlichen Verbesserungsprozess voraus. Die Erfahrungen von Vorgänger- oder parallel laufenden Projekten sollten dabei ebenso einbezogen werden, wie die Informationen von Feldbeobachtungen, wie etwa vom *Cybersecurity Monitoring und Event Assessment,* s. unten.

Information Sharing

Unter welchen Bedingungen können oder müssen Informationen über Bedrohungen und Schwachstellen innerhalb und außerhalb des Unternehmens zur Verfügung gestellt werden?

Die Vorgaben und Vorgehensweisen für das Offenlegen von Schwachstellen und der Weitergabe an betroffene Parteien müssen vom Security-Management erarbeitet und festgelegt werden. In der Vergangenheit hat es sich grundsätzlich als lohnend herausgestellt, wenn securityrelevante Informationen – unter Wahrung der Vertraulichkeit und dem Schutz von Firmengeheimnissen – zwischen den jeweiligen Akteuren ausgetauscht wurden. Diese Idee wurde mit dem Auto-ISAC, dem sog. Automotive Information Sharing und Analysis Center, institutionalisiert. Die Mitglieder und Partner, überwiegend OEMs und Zulieferer der Automobilindustrie, profitieren dabei von der

Stärke der Gemeinschaft. Was sie eint, ist der gemeinsame Feind. Indem sie relevante Informationen über Angriffe, Schwachstellen und Bedrohungen teilen, gemeinsame Lösungen erarbeiten und sich gegenseitig beraten und unterstützen, schaffen sie nicht nur gegenseitiges Vertrauen, sondern sie reduzieren insgesamt auch das Risiko, Opfer eines Angriffs zu werden. Und nebenbei teilen sie sich die Kosten für übergreifende Aufgaben wie etwa des Vulnerability Monitorings.

ISMS
Information Security Management Systeme (ISMS) werden von Unternehmen auch unabhängig von Cybersecurity benötigt, z. B. für den Schutz von Firmengeheimnissen, Geschäftsplänen, Kundendaten, etc. ISMS sind in ISO 27000 standardisiert und in den Unternehmen seit geraumer Zeit etabliert. Die Herausforderung besteht darin, die externe, produktorientierte Sichtweise des CSMS und die nach innen gerichtete Sichtweise des ISMS innerhalb des Unternehmens zusammenzuführen, sowie Gleichanteile bezogen auf Stakeholder, Rollen und Schnittstellen zu identifizieren und sinnvoll miteinander zu verknüpfen.

Risikomanagement
Sind die von Cybersecurity-Bedrohungen stammenden Risiken mit den Unternehmensrisiken abgestimmt?

Die Integration der Cybersecurity-Risiken in das Ensemble der unternehmerischen Risiken ist wie ein zweischneidiges Schwert. Zum einen erhält das Management ein vollständigeres Bild von der aktuellen und tatsächlichen Risikosituation. Die Konsolidierung aller relevanter Informationen erhöht hierbei die Transparenz innerhalb des Unternehmens. Zum anderen ermöglicht dies eine präzisere Planung geeigneter Maßnahmen.

Audit und Zertifizierung
Die UNECE fordert die *Zertifizierung* des CSMS durch einen unabhängigen Auditor als Voraussetzung für die Typenzulassung für Fahrzeuge. Im Audit wird geprüft, ob die umgesetzten Prozesse des CSMS (bzw. des SUMS) den Vorgaben der UNECE WP.29 entsprechen.

Fortlaufende Cybersecurity-Aktivitäten
UNECE WP.29 fordert in R.155 von den Fahrzeugherstellern einen Nachweis darüber, dass das jeweilige, implementierte CSMS geeignete Prozesse für die Überwachung der Fahrzeuge beinhaltet. Diese Überwachung (engl. monitoring) soll fortwährend in der Lage sein, mögliche Bedrohungen und Angriffe auf alle Fahrzeuge im Feld zu erkennen. Außerdem muss das CSMS Prozesse für die Auswertung und Analyse sog. Cybersecurity-relevanter Vorfälle und Schwachstellen definieren.

ISO 21434 sieht hierfür verschiedene Prozesse bzw. Aktivitäten vor. Das Cybersecurity Monitoring erfasst von internen und externen Quellen zunächst alle security-relevanten Informationen und führt eine Eingangsanalyse bzgl. ihrer grundsätzlichen

Relevanz und Korrektheit durch. Das Auto-ISAC stellt etwa eine wichtige externe Quelle dar, wohingegen Security-Untersuchungen interner Spezialisten sowie das sog. *Security Operations Center* (SOC) häufige interne Quellen sind – insbesondere zur Erfassung und Überwachung sämtlicher Fahrzeugdaten und -zustände (field monitoring), s. *Hintergrundinformationen zu SOC*. Im anschließenden Event Assessment wird u. a. mittels einer Schwachstellenanalyse überprüft, ob das Security-Event für das jew. Produkt bzw. Fahrzeug relevant ist und eine mögliche Bedrohung darstellt. Im darauffolgenden Incident Response Prozess wird anhand einer Risikobewertung entschieden, wie auf den Vorfall reagiert werden soll. Wie wird das Problem behoben bzw. der korrekte Systemzustand wiederhergestellt? Welche Maßnahmen müssen getroffen werden, um die Schwachstelle zu beseitigen, bzw. das Risiko auf ein akzeptables Niveau abzusenken? Außerdem ist im sog. *Incident Response Plan* definiert, welche internen und externen Ansprechpartner bei einem Security-Vorfall informiert werden müssen – beispielsweise der Kunde oder das Auto-ISAC. Was UNECE allerdings (noch) nicht vorschreibt, ist die Dauer, d. h. wie lange ein OEM seine Fahrzeuge überwachen muss und auf eventuelle Vorfälle reagieren muss.

Hintergrund

Security Operations Center (SOC)

Das von UNECE WP.29 R.155/R.156 geforderte Cybersecurity-Management, das sich über den gesamten Produktlebenszyklus erstreckt, sieht auch die Überwachung und Wartung der sich im Feld befindlichen Fahrzeuge vor. Ein *Security Operations Center* (SOC) dient dazu, das Einsammeln und Zusammenführen securityrelevanter Informationen, deren Analyse und die Reaktion auf erkannte Angriffe oder zu korrigierende Schwachstellen zentral zu koordinieren.

Die drei wesentlichen Aufgaben eines SOCs sind:

1. Das Erfassen verschiedener interner und externer Informationen, wie etwa Meldungen über neue, bislang unbekannte Schwachstellen in Software-Bibliotheken oder Hardware-Komponenten.
2. Das Verarbeiten dieser Informationen sowie das Erkennen von Angriffen und Analysieren verwendeter Angriffsvektoren.
3. Die Reaktion auf erkannte Angriffe und Schwachstellen, d. h. das Einleiten von Gegenmaßnahmen bzw. das Beheben von Sicherheitslücken.

Vor dem Einzug (breitbandiger) Internetverbindungen in die Fahrzeuge bestand nur die Möglichkeit, securityrelevante Informationen über mögliche Angriffsversuche im begrenzten Umfang in manipulationssicheren Speichern, sog. Security-Logs, der ECUs abzuspeichern und dann etwa im Rahmen von Werkstattbesuchen auszulesen und an das OEM-Backend zu Analysezwecken zu übermitteln. Eine unmittelbare oder kurzfristige Reaktion auf einen erkannten Angriff war nicht möglich.

Bei Fahrzeugen, die über eine Internetverbindung verfügen, können securityrelevante Informationen regelmäßig und oftmals auch in größeren Mengen an das

zentrale Backend übermittelt werden. In der Gegenrichtung können vom Backend *Software- und Policy-Updates* an die Fahrzeuge verteilt werden.

Ein zentrales Monitoring-System, das regelmäßig mit aktuellen Informationen über Cybersecurity-Events versorgt wird, birgt gegenüber kleineren, dezentralen Lösungen oder sogar den (historischen) Offline-Lösungen, s. oben, mehrere Vorteile.

Zum einen erlaubt die Überwachung der gesamten Fahrzeugflotte eines OEMs und bestenfalls der Zusammenschluss mit anderen Vertretern der Branche eine bessere und frühzeitige Erkennung von Angriffsmustern und Anomalien. Die Bündnispartner können sich gegenseitig vor Angriffen warnen.

Zum anderen verschafft der Informationsaustausch über Schwachstellen und Angriffe den Partnern dieser Allianz einen entscheidenden Vorsprung gegenüber den Bedrohungen der dunklen Seite. Deren Vertreter, etwa mutmaßliche Angreifer und Black-Hat-Hacker, teilen bzw. verkaufen ihre Informationen über mögliche Angriffsvektoren typischerweise in verschiedenen Foren und Kanälen des Internets. Das Aufklären und Verfügbarmachen dieser Informationen über mögliche Bedrohungen, die sog. *Threat Intelligence*, kann in der Zusammenarbeit und mit gemeinsamen Ressourcen besser gelingen.

Wie ist ein SOC informationstechnisch angebunden?

Welche Informationen benötigt ein SOC? Welche Informationen bzw. Erkenntnisse erzeugt ein SOC?

Die Aufgabe (1), s. oben, besteht im Zusammentragen aller relevanter Informationen über Cybersecurity-Events. Dabei werden sowohl externe als auch interne Informationsquellen einbezogen.

Zu den externen Informationsquellen zählen:

- Auto-ISAC: Informationsaustausch und Reportings bzw. Alerts
- Internet, öffentliche Datenbanken über Security-Schwachstellen (z. B. *cve.mitre.org*), einschlägige Web-Foren und Social-Media-Kanäle
- Informationen von Security-Dienstleistern und entgeltliche Dienste von Drittanbietern
- *Bug-Bounty-Programm*: Beschaffung von Informationen von White-Hat-Hackern durch Auslobung von Preisgeldern

Zu den internen Informationsquellen zählen:

- Die eigene Fahrzeugflotte: Das *Intrusion Detection System* (IDS), s. Abschn. 5.3.3, stellt eine der wichtigsten Informationsquellen dar. Die begrenzten Ressourcen der Intrusion Detection Systeme im Fahrzeug sowie der fehlende Informationsaustausch mit anderen Fahrzeugen erlauben allerdings nur einfache Analysen sowie das Herausfiltern irrelevanter Informationen.
- *Honeypots,* können sowohl in Fahrzeugen als auch in der Backend-IT-Infrastruktur, als Lockvogelsystem die Aufmerksamkeit der Angreifer auf sich ziehen. Ein Angriff

auf einen Honeypot dient neben der Vorwarnung auch als Informationsquelle, um Technik und Methodik der Angreifer zu untersuchen.
- Interne Security-Reviews und Penetrationstests, u. a. vom eigenen Red Team, sind ebenfalls ein probates Mittel, um Schwachstellen und Sicherheitslücken zu identifizieren oder bestenfalls auch auszuschließen.
- Security-Event-Informationen vom IT-SOC des Unternehmens sollten ebenfalls mit den Informationen des (Fahrzeug-)SOCs abgeglichen werden.

Die Aufgabe (2) besteht zunächst in der *Vorverarbeitung* der gesammelten Informationen. Bestimmte Informationen wie etwa personenbezogene Daten, werden ggf. gefiltert oder pseudonymisiert. Falsch-positive Meldungen müssen idealerweise automatisiert herausgefiltert werden. Im Anschluss erfolgt die Analyse: Die Daten der verschiedenen Datenquellen werden konsolidiert und ggf. miteinander abgeglichen. Gibt es Zusammenhänge zwischen bestimmten Cybersecurity-Events im Backend und in den Fahrzeugen? Sind bestimmte Muster oder Wiederholungen erkennbar? Gibt es Anzeichen für großflächige Angriffe?

Der bereits erwähnte Vorteil des zentralen Monitorings im Backend ist die quasi beliebig große bzw. leicht skalierbare Rechenleistung, was u. a. die Verarbeitung größerer Datenmengen und damit komplexe Analysen und Schlussfolgerungen möglich macht. Ziel ist es, Angriffe und Versuche zu erkennen und zu verstehen. Die Angriffspfade müssen nachvollziehbar sein und ggf. rekonstruiert werden. Aus den gewonnenen Erkenntnissen können ggf. Empfehlungen für Abhilfemaßnahmen abgeleitet werden.

Die Aufgabe (3) besteht im Anstoßen der (Gegen-)Reaktion auf erkannte Angriffe und Sicherheitslücken. An diesem Punkt werden Gegenmaßnahmen definiert und ggf. werden Software-Updates erstellt und per (OTA-)Update ausgerollt. In diesem Zuge werden ggf. auch Policies und Strategien für IDS, Firewall etc. nachgeschärft und auf die neuen Bedrohungen angepasst.

Wie ist ein SOC prozesstechnisch angebunden?

Das SOC stellt ein essenzielles Element für das Cybersecurity-Monitoring in der Post-Produktionsphase dar. Mit seinen Aufgaben ist es mit verschiedenen Teilprozessen verknüpft, u. a. mit dem *Cybersecurity Event Monitoring* und *Vulnerability Monitoring,* dem *Event Assessment,* dem *Incident Response Prozess* sowie dem Update-Prozess als Werkzeug um Gegenmaßnahmen und Korrekturen bzw. vorbeugende Maßnahmen kurzfristig im Feld flächendeckend auszurollen.

Die Zusammenarbeit und der reibungslose Informationsaustausch zwischen den beteiligten Teams (z. T. auch Teams verschiedener Unternehmen) ist unabdingbar, um schnell und effizient gegen eine Bedrohung reagieren zu können. Die folgenden Personengruppen sind bei den oben genannten Aufgaben involviert:

- Security Experten der jew. Entwicklungsabteilungen
- PSIRT-Team(s)

- IT-Security-Teams (CSIRT, etc.)
- ext. Partner wie etwa ISAC-Analysten◀

Operations and Maintenance
Neben dem oben umrissenen Incident Response Management definiert ISO 21434 auch die Möglichkeit, Fahrzeuge in der Post-Produktionsphase aktualisieren zu können, s. Abschn. 5.5.4. Diese Fähigkeit ist eine zentrale Anforderung von UNECE WP.29 R.156, s. oben.

Verteilte Cybersecurity-Aktivitäten
ISO 21434 sieht auch vor, bestimmte Verantwortlichkeiten zu übertragen. In einer dafür vorgesehenen Schnittstellenvereinbarung werden verantwortliche, mitarbeitende und zu informierende Parteien definiert. Im Gegensatz zum Zuschneiden der Prozesse (Tailoring) werden hierbei keine Aktivitäten weggelassen oder modifiziert ausgeführt, sondern lediglich einer anderen Rolle bzw. Person zugewiesen. Ein allseitiges Verständnis der Anforderungen ist eine zwingende Voraussetzung und muss ggf. vom Security-Management sichergestellt werden.

Zusammengefasst: Die Anforderungen der UNECE WP.29 bzw. des ISO 21424-Standards an das Cybersecurity Management betrifft mehrere Bereiche der Organisation:

- Die Unternehmensführungen sind für die strategischen Vorgaben, die Security-Kultur und das Risikomanagement verantwortlich.
- Die Personalabteilung ist für den Aufbau der Securityteams sowie für die Schulungs- und Weiterbildungsmaßnahmen zuständig.
- Die Rechts- und Qualitätsabteilungen vertreten Compliance- bzw. Zertifizierungsthemen.
- Die IT-Security-Teams sind insbesondere beim Aufbau und Betrieb von Backend-Komponenten wie SOC, OTA-Update-Server, etc. involviert. Außerdem ist ihre Expertise im Bereich des Informationsschutzes gefragt.
- Die Entwicklungsabteilung ist verantwortlich dafür, dass Cybersecurity *by-design,* d. h. von Anfang an durchgehend in der Produktentwicklung berücksichtigt wird.

Literatur

1. UNECE. (2021a). UN Regulation No. 155 – Cyber security and cyber security management system | UNECE. UNECE.ORG. https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security. Zugriffsdatum 2021-06-01.
2. UNECE. (2021b). UN Regulation No. 156 – Software update and software update management system | UNECE. UNECE.ORG. https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update. Zugriffsdatum 2021-06-01.