CYBERSICHERHEIT VON FAHRZEUGEN

Angriffserkennung und -abwehr für permanenten **Cyberschutz**

Angesichts zunehmender Vernetzung und Automatisierung der Fahrzeuge sowie neuer Regulierungen müssen OEMs ihre Fahrzeugflotten künftig über den gesamten Lebenszyklus vor Cyberattacken schützen. Statt Symptombekämpfung durch einzelne Security-Maßnahmen ist umfassender Immunschutz in Form einer „Intrusion Detection and Prevention Solution" (IDPS) gefragt.

Spätestens mit den in 2020 verabschiedeten UN-Regulierungen UN R155, UN R156 ist die Cybersicherheit der Fahrzeuge für OEMs und Zulieferern zur Schlüsseltechnologie geworden. Insbesondere Annex 5 der UN R155 listet explizit die zu betrachtenden Schwachstellen und Bedrohungen (Teil A) auf sowie auch technische Maßnahmen zu deren Mitigation, sprich zur Minderung des Risikos (Teile B, C). Bezeichnenderweise finden sich in Teil B des Annex 5 gleich eine ganze Reihe zu berücksichtigender Mitigationen, die einer funktionierenden Angriffserkennung im Fahrzeug bedürfen. Mitigation M15 etwa verlangt nach „Maßnahmen zur Erkennung maliziöser interner Nachrichten oder Aktivitäten", M9 nach „Maßnahmen zur Verhinderung und Aufdeckung von unbefugtem Zugang" – die Liste ließe sich erweitern [1].

Die UN R155 folgt hier dem für die Produktsicherheit bewährten „Defense-in-Depth"-Ansatz, bei dem die Angriffserkennung möglichst tief und mannigfach ins Fahrzeug und sein internes Netzwerk eingebettet sein sollte [2]. Nur so lassen sich auch lokale Angriffe mit physischem Zugriff, beispielsweise über das Diagnose-Interface oder die USB-Schnittstelle des Infotainmentsystems erkennen oder auch Chip-Tuning oder Ad-Blue-Manipulation durch den Fahrzeughalter erfassen.

Netzwerk-IDS vs. Host-basiertes IDS

Je nachdem, auf welcher Ebenen im Fahrzeug die Angriffserkennung erfolgen soll, wird dafür auf Netzwerk- oder Host-basierte Intrusion Detection Systeme (Network IDS vs. Host-based IDS) zurückgegriffen, die sich jeweils unterschiedlicher Technologie-spezifischer IDS-Sensoren bedienen. Netzwerk-IDS verfügen über ein breiteres „Blickfeld", im besten Fall sogar über alle Fahrzeugnetze hinweg. Entsprechend lassen sich ihre Sensoren flexibel anordnen, beispielsweise auf den vermeintlich am besten gegen Zugriffe geschützten Fahrzeugsteuergeräten (ECU). Allerdings erkennen sie – außer bei Angriffen über

offene Schnittstellen – die Cyberattacke oder Manipulation erst, wenn die angegriffene ECU bereits kompromittiert ist. Anders bei den Host-basierten IDS: Diese werden typischerweise ECU-spezifisch implementiert und verfügen entsprechend nur über ein lokales, auf die einzelne ECU begrenztes „Blickfeld". Ihr Vorteil jedoch: Host-basierte IDS-Sensoren erkennen den Angriff auf die ECU bereits in dem Moment, in dem er erfolgt.

Host-basierte und Netzwerk-IDS schließen sich nicht aus, sondern können auch zielführend miteinander kombiniert werden. Entscheidendes Kriterium bei der Wahl der IDS-Sensoren sollte immer sein, dass diese Technologie-spezifisch auf die E/E-Architektur des Fahrzeugs hin optimiert sind, z.B. was den Grad ihrer Einbettung, ihren Ressourcenbedarf sowie Qualitäts- und Prozesserfordernisse fahrzeuginterner Netzwerke angeht. Zudem sollten die eingesetzten IDS-Sensoren speziell auf die Automotive-Kommunikationsstandards hin entwickelt worden sein – sei es CAN oder Automotive Ethernet.

Verteiltes IDS als Nervensystem des Fahrzeugs

Die verteilten IDS-Sensoren fungieren in Bezug auf etwaige Cyberangriffe, unerlaubte Zugriffe und Manipulationen wie „Synapsen im Nervensystem des Fahrzeugs". Sie melden Anomalitäten im Netzwerkverkehr oder maliziöse Diagnoseanforderungen weiter an den IDS-Manager (IdsM), von wo aus die konsolidierten Logfiles an den IDS-Reporter (IdsR) zwecks Upstream ans Backend übergeben werden. Wichtig dabei: In all diesen drei Instanzen des Intrusion-Detection-Systems muss das Regelwerk konsistent abgebildet sein; nur dann sind optimale Implementierung, Erkennungsgenauigkeit und Wirksamkeit des vernetzten Systems gewährleistet (Bild 1).

Gleichzeitig gilt es, so früh wie möglich die Datenmenge zu reduzieren. Aufgrund begrenzter Bandbreiten und Ressourcen für den Datentransfer und im Backend ist es sinnvoll, bereits im Fahrzeug über smarte IDS-Sensoren und IDS-Manager falsch-positive Security-Events, nicht relevante Events bzw. Rauschen herauszufiltern. Dabei muss jedoch im Sinne einer effektiven Ende-zu-Ende-Security dem Verlust relevanter Informationen vorgebeugt sein; die Optimierung der Datenmenge darf nicht zu Lasten der Erkennung gehen.

V-SOC: Kommandostand fürs flottenweite Monitoring

Indes ist für eine ganzheitliche Intrusion Detection & Prevention Solution (IDPS) Erkenntnis nur der erste, wenngleich wichtige Schritt. So unverzichtbar die Angriffserkennung im einzelnen Fahrzeug, so wichtig ist die Zusammenführung und Verarbeitung der Event-Daten für die vernetzten Fahrzeugflotte im Vehicle Security Operations Center (V-SOC) im Backend, das als zentraler Taktgeber einer Regelschleife aus Monitoring, Detection, Analysis, Response und Prevention wirkt. Mit seinem maßgeblichen Ziel eines proaktiven Security-Monitorings wird das V-SOC quasi zum Kommandostand eines solchen Regelkreises – und setzt dabei auf das Zusammenwirken von drei Komponenten:

- Eine Software-Plattform, die Daten aggregiert und zielführend verarbeitet – Aufgaben der V-SOC-Plattform sind dabei insbesondere das Filtern von Falschmeldungen (false positives), die automatische Klassifikation von Events, die automatisierte Verarbeitung von bereits bekannten Ereignissen sowie die Vorverarbeitung, Aufbereitung und Zusammenfassung (Clustering) von Daten für eine effiziente Bearbeitung durch Analysten.
- Prozesse, die die Bearbeitung der Security-Events sicherstellen und steuern – Prozessual ist im V-SOC sicherzustellen, dass kritisch bewertete Security-Vorkommnisse bearbeitet werden. Dies umfasst eine Aufbereitung mit relevanten (und verfügbaren) Hintergrundinformationen und eine Ableitung von Hand-

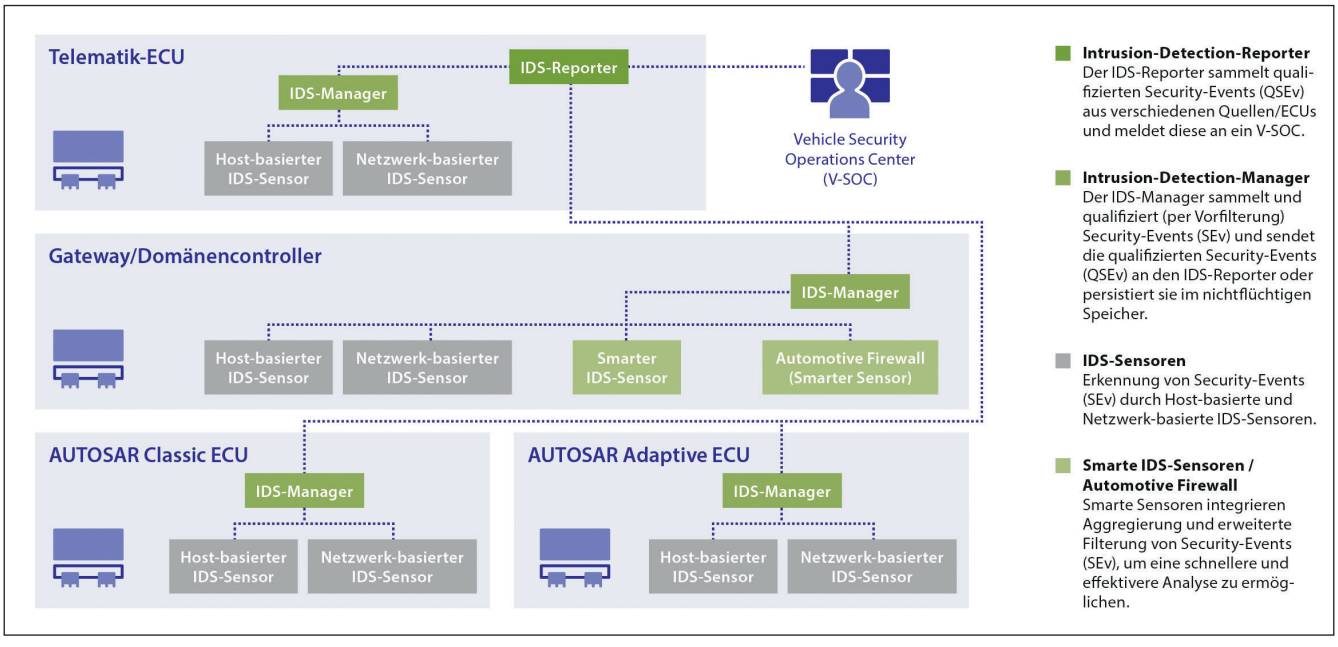

Bild 1: Architektur eines verteilten Intrusion-Detection-Systems (IDS) im Fahrzeug – vom (smarten) IDS-Sensor über den IDS-Manager zum IDS-Reporter. © ESCRYPT

lungsempfehlungen. In dieser Weise werden die Events in ein verständliches, handlungsorientiertes Reporting und letztlich in ein Security-Lagebild überführt, das erlaubt, Schwachstellen und Risiken zu erkennen und regulatorische Anforderungen zu erfüllen.

- Analysten, die die Daten darüber hinaus manuell untersuchen, bewerten und bearbeiten. Die Automotive-Security-Analysten im V-SOC unterstützen bei der genaueren Untersuchung von Vorkommnissen und sorgen dafür, dass Incident-Management-seitig die notwendigen Maßnahmen abgeleitet werden, um kritischen Ereignissen wirksam zu begegnen.

können Daten aus den zum Fahrzeug-Backend gehörenden IT-Systemen mit in die Analyse miteinbezogen werden, insbesondere dort, wo Fahrzeugfunktionen (z.B. per Smartphone-App) über solche Backend-Systeme kontrolliert werden. Entsprechend müssen all diese Automotive-spezifischen Daten gemäß V-SOC-eigenen Aggregationsregeln und eigener Datenlogik aufbereitet werden (Bild 2).

Doch nicht nur technologisch gilt es, Security- und Automotive-Know-How im V-SOC zu vereinen. Es sind Analysten gefragt, die einerseits über ein gutes Verständnis hinsichtlich Erkennung und Management von Security-Vorfällen verfügen, die aber auch spezielles Automotive-Domänen-Wissen mitbringen und z. B. fachgerecht beurteilen können, ob eine Meldung oder eine Anomalie tatsächlich auf einem mutwilligen Eingriff

che Daten zwingend in einem Monitoring zu betrachten sind. Auch eine „Automotive Threat Intelligence", welche Erkenntnisse aus konkreten Vorfällen nutzt, um die Analyse in anderen Fällen zu leiten und zu optimieren, ließe sich herstellerübergreifend organisieren. Bestenfalls greift diese dann auf Quellen zurück, die domänenspezifische Angriffsmuster aus dem Automobilbereich zusammenführen, sowie auf gemeinsame Formate, um diese Informationen auszutauschen.

Selbst bei den Response-Optionen ließen sich über gemeinsame Standards neue Wege erschließen. Anstatt auf erkannte Sicherheitslücken nur mit dem Ausrollen von Sicherheits-Updates oder Rekonfigurationen in Fahrzeugen zu reagieren, wären – speziell auch mit Blick auf das automatisierte Fahren – standardisierte Rückfallebenen denkbar, die als

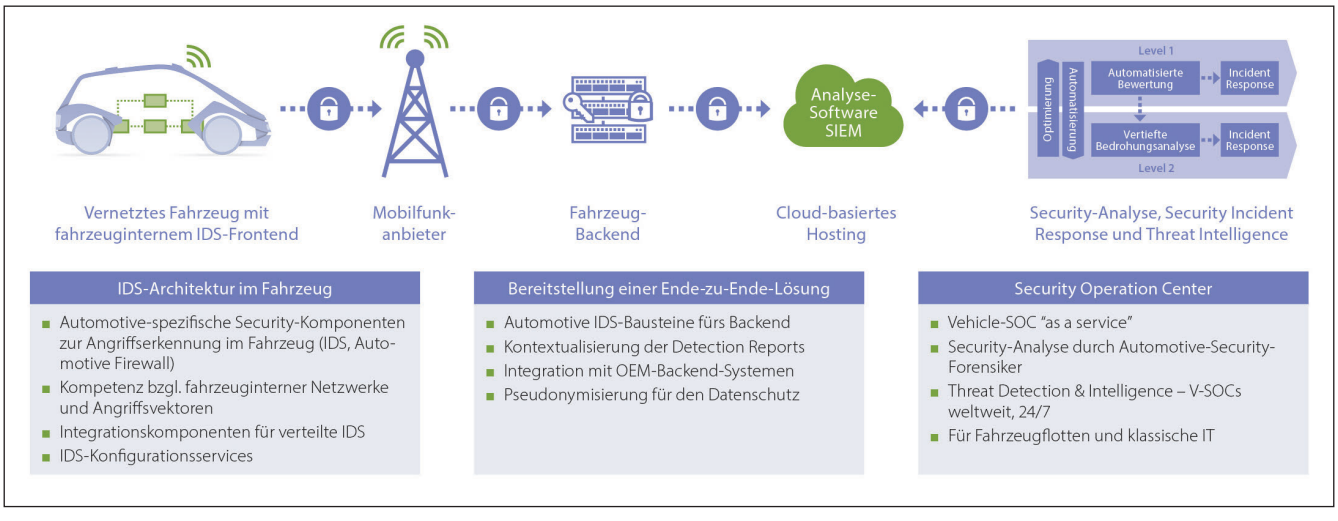

Bild 2: Vehicle Security Operations Center im Zusammenspiel mit der Angriffserkennung im Fahrzeug. © ESCRYPT

Spezifische Use Cases, qualifizierte Analysten

Im Gegensatz zu einem Security Operations Center (SOC) für klassische Unternehmens-IT muss ein V-SOC auf die speziellen Anwendungsfälle im Automotive-Bereich zugeschnitten sein. Die potenziellen Bedrohungen sind zum Teil andere als in der klassischen Enterprise-IT (z.B. Fault-Injection-Angriffe). Auch die Quellen der Daten, die einer Analyse zugeführt werden, unterscheiden sich. Da sind zum einen die IDS-Logfiles aus den Fahrzeugen, aber auch Flotten- und Fahrzeugdaten, die bei den OEMs und Flottenbetreibern verfügbar sind, zum Beispiel aus Telematiksystemen. Zudem

basiert oder eine tolerierbare Falschmeldung ist. Der Schlüssel für ein erfolgreiches V-SOC liegt demnach in der Zusammenarbeit von Security- und Domänen-Experten – auch um das Domänenwissen nach und nach in die Optimierung der Plattform und der Abläufe einzubringen.

Herstellerübergreifende Zusammenarbeit

Wünschenswert wären industrieweit einheitliche Standards für die Überwachung von Fahrzeugflotten mittels V-SOC. So könnten etwa für standardisierte Anwendungsfällen klare Mindestanforderungen formuliert werden, wel-

Reaktion auf erkannte Sicherheitsvorfälle im Fahrzeug ausgelöst werden können.

Response per Update und SUMS

Tatsächlich ist die Response wesentlicher Baustein im Zyklus des kontinuierlichen Risikomanagements. Denn während Security-Mechanismen, Algorithmen und Kryptoverfahren über die Lebensdauer der Fahrzeuge hinweg veralten, bedienen sich Angreifer immer neuer Angriffstechniken. Software-Updates sind ein probates Mittel, um erkannte Schwachstellen zu schließen und den „Prevention Status„, den hinreichenden Schutz des Fahrzeugs, wiederherzustel-

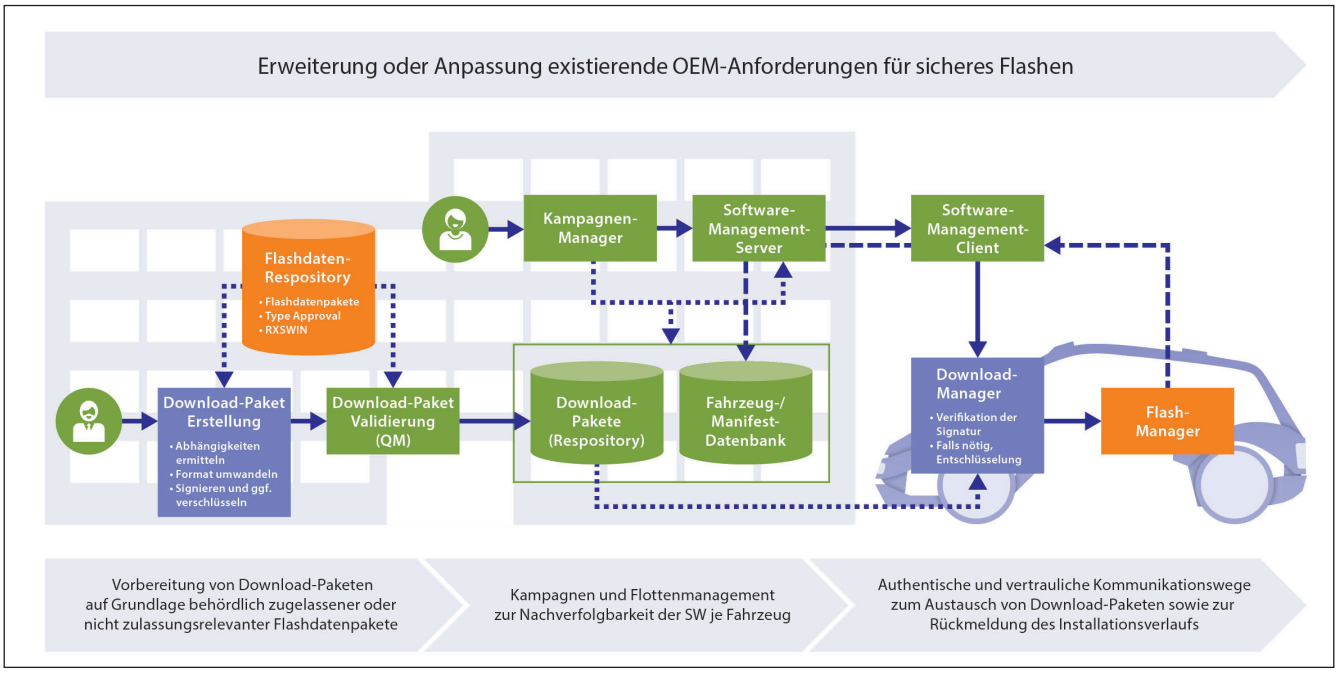

Bild 3: Software-Update-Managementsystem (SUMS) – Sicheres Ausrollen und Installation von Software-Update-Paketen. © ESCRYPT

len. Dabei lassen sich konventionelle Updates in der Werkstatt in zunehmendem Maße durch Over-The-Air(OTA)-Systeme ergänzen oder gar ersetzen. Die Update-Frequenz kann so beliebig verkürzt, die Kosten reduziert werden.

Es bedarf demnach künftig eines Software-Update-Managementsystems (SUMS), welches die Aufbereitung und Verteilung von Software-Updates für die Flotte entlang festgeschriebener Prozesse organisiert. Gemäß UN R156 adressiert ein solches SUMS u.a. die Weitergabe von Informationen an OEMs oder Zulassungsbehörden, die Identifikation typgenehmigungsrelevanter Softwareanpassungen, die Nachverfolgbarkeit von Änderungen, mögliche Interdependenzen aktualisierter Systeme, die Integrität und Authentizität der Software-Updates, die Funktionssicherheit des Fahrzeuges oder auch den Umgang mit fehlgeschlagenen Updates [3].

Authentizität der Updates

Wichtigstes „Security Goal" ist es, die Integrität und Authentizität der Updates sicherzustellen. Es gilt zu verhindern, dass Update-Mechanismen missbraucht werden, um Steuergeräte oder andere Instanzen im fahrzeuginternen Netzwerk anzugreifen, zu manipulieren oder zu deaktivieren. Ein Firmware-Over-The-Air(FOTA)-Update muss daher entlang folgender drei Erfordernisse konzipiert sein (Bild 3):

- Authoring-Security-Prozesse: Es braucht einen klar definierten Prozess der Mandatierung für FOTA-Update-Pakete. Die von OEM-eigenen Entwicklern bzw. von Zulieferern erstellten Updates werden ausschließlich von eigens autorisierten Stellen mit digitaler Signatur freigegeben.
- Backend-Security-Konzept: Das Backend selbst muss per Defense-in-Depth-Ansatz so abgesichert sein, dass unerlaubte Zugriffe auf validierte Update-Pakete nicht möglich sind.
- In-Vehicle-Security-Konzept: Im Fahrzeug muss geprüft werden, ob die Quelle des Updates authentisch ist (Verifikation der digitalen Signatur), ob das aktuelle Manifest mit dem Inhalt des Pakets übereinstimmt und ob für die Installation des Updates ein bestimmter Fahrzeugzustand erforderlich ist (z. B. geparkter Zustand beim Software-Update für Motorsteuerung).

Gefordert ist ein ganzheitliches Cybersicherheitssystem, das geeignet ist, neuen Angriffstechniken und sich stetig ändernde Gefahrenlagen rasch neue, geeignete Schutzmechanismen entgegenzusetzen. Auf solch einen weitgehenden, kontinuierlichen „Immunschutz" zielt IDPS. Die Intrusion Detection & Prevention Solution vereint die Angriffserkennung im Fahrzeug mit Überwachung, Analyse und Herleitung notwendiger Gegenmaßnahmen im Backend und einem OTA-Software-Update-Management als „Impfkampagne" für die Flotte. ■ (oe)

www.escrypt.com

Literatur & Links

[1] UNECE World Forum for Harmonization of Vehicle Regulations: Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. Unter: http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29–2020–079-Revised.pdf

[2] Ramona Jung. Ohne Security keine Safety. ATZextra Automatisiertes Fahren, März 2019.

[3] UNECE World Forum for Harmonization of Vehicle Regulations: UN Regulation No. 156 – Software update and software update management system. Unter: https://unece.org/sites/default/files/2021–03/R156e.pdf

Dr. Jens Gramm ist Senior Product Manager Vehicle Security Operations Center bei ESCRYPT am Standort Stuttgart.

Dr. Jan Holle ist Lead Product Manager Intrusion Detection & Prevention Solution bei ESCRYPT am Standort Stuttgart.

Dipl.-Ing. Thomas Stimm ist Security Engineer bei ESCRYPT am Standort Bochum.