© Shutterstock.com | Gorodenkoff, ESCRYPT

VEHICLE SECURITY OPERATIONS CENTER

Die Fahrzeugflotte permanent im **Blick**

Angesichts immer neuer Angriffstechniken, benötigen Fahrzeugflotten künftig eine fortwährende Überwachung und Absicherung. Dies begründet sich vor allem durch das neue UN-Regelwerk zu Cybersicherheit und Software-Updates. Entscheidend dabei: Das Zusammenwirken zwischen Angriffserkennung im Fahrzeug und SIEM, Threat Intelligence und Security-Analysten im Vehicle Security Operations Center.

Egal wie hoch das Schutzlevel vor Cyberangriffen, das bei der Entwicklung geschaffen wurde, auch ist, es wird über die Lebensdauer des Fahrzeugs hinweg zwangsläufig erodieren. Neue Sicherheitslücken werden entdeckt und ausgenutzt, neue Angriffsmethoden und -werkzeuge entwickelt, über die Zeit lassen sich einzelne Schwachstellen womöglich zu einer Kill Chain vervollständigen.

In Zeiten vernetzter Mobilität trifft das Problem OEMs, Flottenbetreiber und Managed Service Provider (MSP) gleichermaßen. Umso mehr als Angriffe – ganz gleich, ob nur versucht oder erfolgreich – häufig unentdeckt bleiben. Denn von gängiger Onboard-Diagnosetechnik werden Cyberangriffe nicht erfasst. Die Analyse und Reproduktion etwaiger Attacken ist daher schwierig und teuer, eine zeitnahe Reaktion kaum möglich. Was bleibt ist der Schaden: Negative Folgen für Fahrzeug, Fahrzeugnutzer und andere Verkehrsteilnehmer sowie Reputationsverlust und Folgekosten für OEMs, Flottenbetreiber und MSPs.

Fortlaufende Überwachung der Fahrzeugflotte

Genauso wie heute IT-Systeme im Unternehmen einer fortlaufenden Überwachung hinsichtlich verdächtiger Vorgänge und möglicher Cyberangriffe unterzogen werden, benötigen daher künftig auch Fahrzeug und Fahrzeugflotten ein aktives, fortwährendes Security Monitoring. Dabei geht es zum einen um die Überwachung bekannter Risiken, etwa indem die Ausnutzung bereits bekannter Angriffsvektoren kontinuierlich beobachtet wird. Zum anderen zielt ein solches Security Monitoring auf die Identifikation neuer Risiken. Es erkennt, welchen Angriffen die Fahrzeuge im Feld ausgesetzt sind und welche neuen Methoden Angreifer ausprobieren, so dass bereits frühzeitig – noch bevor die Angreifer ihre Attacken skalieren – Gegenmaßnahmen eingeleitet werden können.

Ziel einer solchen permanenten Überwachung ist es, das Security Level des Fahrzeugs fortlaufend und anforderungsgerecht nachzubessern. Das ganzheitliches Vehicle Security Operations Center (V-SOC) von Escrypt folgt hierbei dem klassischen Zyklus aus Monitoring, Angriffserkennung, Analyse und Response. Es muss demnach nicht nur

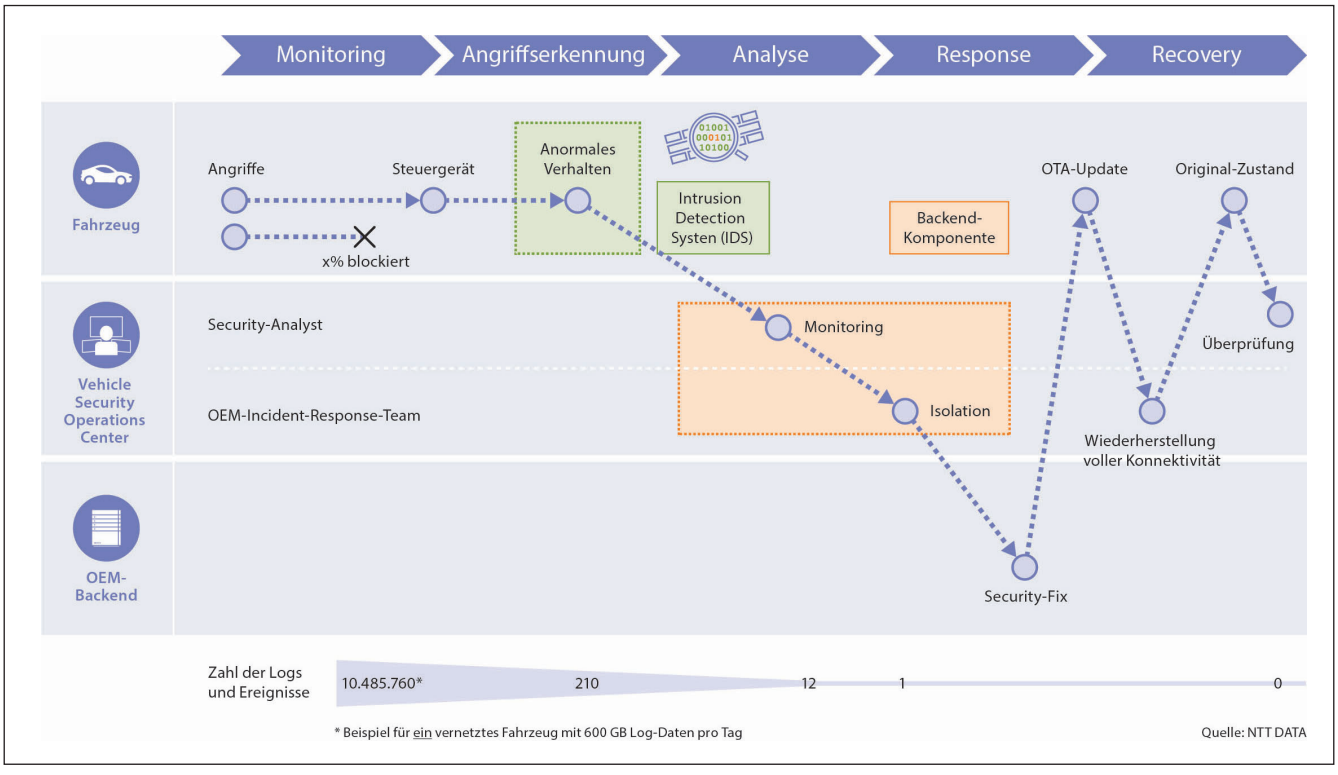

Bild 1: Security Incident Management Journey – Das IDS erkennt Anomalien und typische Angriffssignaturen in der Fahrzeugkommunikation und reduziert so den Bandbreitenbedarf für die Übertragung der Security Monitoring-Informationen. © NTT DATA, ESCRYPT

den Datenverkehr im, zum und vom Fahrzeug überwachen, sondern auch gleichzeitig Anomalien und mögliche Security Events herausfiltern und melden. Und es benötigt ein Security-Backend, dass diese Auffälligkeiten qualifiziert aus- und bewertet und von dem aus die zur Aufrechterhaltung oder Wiederherstellung des Schutzniveaus nötigen Software-Patches entwickelt und per Software-Update Over-the-Air (SOTA) auf die Flotte ausgerollt werden (Bild 1).

Beobachtung des Gesamtsystems gemäß UNECE-Regularien

Dabei ist ein solcher Regelkreis zur Absicherung der Fahrzeugflotte keineswegs fakultativ. Spätestens mit Inkrafttreten der Regularien der UNECE.WP29, die jüngst von rund 60 Ländern angenommen wurden, wird der Nachweis einer angemessenen Risikobehandlung sowie eines Security Monitorings über den gesamten Fahrzeuglebenszyklus hinweg zur verpflichtenden Voraussetzung für die Typgenehmigung. Einzelne Security-Funktionen im Fahrzeug werden dafür nicht ausreichen, sondern der kontinuierliche Schutz der Fahrzeuge bis zum Phase-out – zwingend bestehend aus Detection und Response – muss organisatorisch, prozessual und technisch unterfüttert und verbürgt sein.

Um ein aussagekräftiges Bild der Gesamtbedrohungslage zu erhalten, ist es nicht sinnvoll, das Beobachtungsfeld lediglich auf die Flotte oder auf das Backend einzuengen. Vielmehr braucht es mehrere Blickfelder und Handlungsebenen gleichzeitig: Ein Monitoring im Fahrzeug in Form eines Intrusion Detection System (IDS), das Angriffe und Manipulationen dort aufspürt, wo sie sich unmittelbar zeigen und wirksam werden, und ein Security Monitoring für das (OEM-)Backend. Sowie überdies ein Security Operations Center (SOC), in dem das Angriffsgeschehen aggregiert und ausgewertet wird, und das eine Skalierung von Angriffen über die ganze Flotte hinweg unterbindet.

Intrusion Detection im Fahrzeug

Das Intrusion Detection System ist demnach von entscheidender Bedeutung für die Effektivität des Security-Monitorings insgesamt. Die Qualität und Zuverlässigkeit der Angriffserkennung im Fahrzeug misst sich dabei an zwei Fragen: Wo im Fahrzeug werden Intrusion-Detection-Systeme (IDS) eingesetzt? Und was genau beobachten diese?

Aktuell geht der Trend dahin, den fahrzeuginternen Datenverkehr (Ethernet, CAN) beobachten zu lassen und zusätzlich IDS in den am meisten exponierten ECUs (Connectivity ECUs) zu platzieren. Ziel der Intrusion Detection ist dabei insbesondere, Angriffe von außen (per Remote Connectivity) frühzeitig zu entdecken, die Manipulation fahrrelevanter Systeme (z. B. Lenksystem, Motorsteuerung) zu erkennen oder auch Manipulationsversuche über leicht zugängliche Schnittstellen (wie z. B. die Diagnoseschnittstelle) zu erkennen.

- Ein Netzwerk-basiertes IDS für den CAN-Bus überwacht den CAN-Traffic bspw. von einem zentralen Gateway aus und analysiert ihn nach regelbasiertem Vorgehen. Die Intrusion Detection erkennt dabei typische CAN-Angriffe, etwa Angriffen auf Diagnoseprotokolle wie UDS oder die Manipulation von CAN-Signalen (Signatur basierter Ansatz) und Anomalien welche auf neue (bisher nicht klassifizierte Angriffe) hindeuten (Heuristischer Ansatz).
- Ein Host-based IDS auf der Connectivity ECU überwacht beispielsweise die Integrität des Betriebssystems und der Anwendungen. Das Intrusion-Detection-System

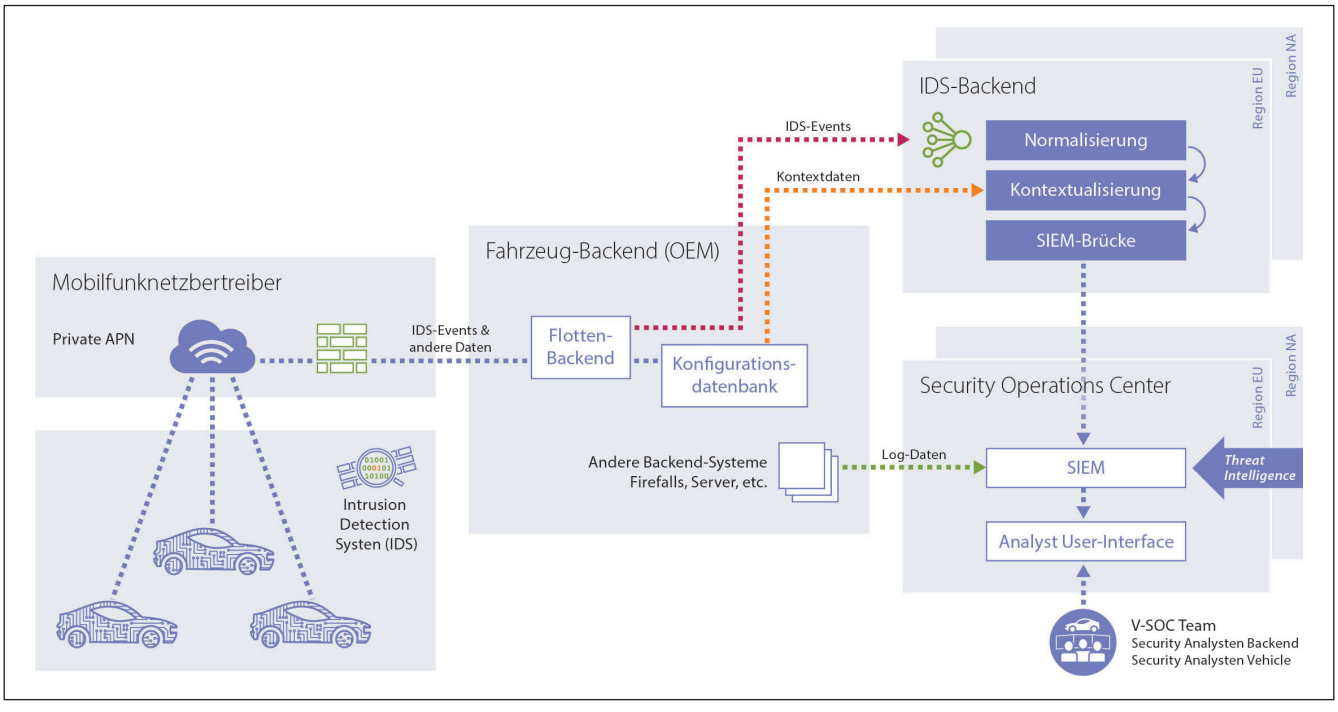

Bild 2: Bestandteile eines ganzheitlichen Vehicle Security Operations Center – Von der Intrusion Detection zum Security Operation Center.

erkennt dabei Veränderungen von System- und Anwendungsdateien und scannt die aus- und eingehenden Netzwerkverbindungen.

- Durch eine Kombination von Host-basierten IDS und netzwerk-basierten IDS entstehen hybride / verteilte IDS, die die Abdeckung der Angriffsfläche im Fahrzeug erhöhen und umfassende Information über das Vorgehen von Angreifern sammeln. Neue AUTOSAR-Module wie der IDS Manager (idsM) ermöglichen die Verteilung, Weiterleitung und Sammlung von Security Events im Fahrzeugnetzwerk bis zur Übergabe an das Backend in einer Connectivity ECU.

Darüber hinaus erbringt das IDS im Fahrzeug einen weiteren entscheidenden Vorteil: Es reduziert den Bandbreitenbedarf für die Übertragung der Security Monitoring-Informationen erheblich. Denn im Gegensatz zum Security Monitoring in der Enterprise-IT, das sich auf breitbandige Netzwerkanbindung stützt und so z. T. den kompletten Netzwerkverkehr mitschneiden und die gesamten Logs der einzelnen Systeme übertragen kann, verfügt die Fahrzeugflotte nur über eine Anbindung mit geringer Bandbreite. Das IDS wirkt hier wie ein Filter – statt des gesamten Datenverkehrs und großer Logs reportet es nur die entdeckten Anomalien an das Backend. Die Menge der zu übertragenden Daten wird dadurch drastisch reduziert.

Security Incident und Event Management (SIEM)

Zentrale Herausforderung bei der Sicherung der Flotte ist es, bislang unbekannte Angriffe frühzeitig zu erkennen. Ein zentrales Werkzeug dabei ist das Security Incident und Event Management (SIEM). Es sammelt – über einen definierten Zeitraum hinweg – alle IT-Sicherheitsereignisse, die die Security-Sensoren im Backend und in den Fahrzeugen melden.

SIEM-Lösungen bringen eine Reihe nützlicher Funktionen mit: Sie werten Logdateien unterschiedlicher Serverprodukte (Firewalls, Proxys, VPN-Appliances, Server und andere Security-kritische Komponenten) aus und bedienen sich dabei der marktüblichen Logformate. Sie sammeln die Logdaten, und unterstützen die Retention alter, nicht mehr benötigter Daten. Zudem hilft das SIEM bei der Analyse der gesammelten Log-Dateien, indem es diese durchsucht, darstellt und mitunter sogar ermöglicht, mittels Machine-Learning-Funktionalitäten eigene Modelle zu entwickeln. Und nicht zuletzt veranschaulichen SIEMs mittels Dashboards die Risikolage und sind vielfach sogar mit Vulnerability-Management-Lösungen kombinierbar.

SIEM: Gut bei bekannten, weniger gut bei unbekannten Angriffen

Um automatisiert bekannte Angriffe zu erkennen, sind SIEMs daher bestens geeignet, zumal sie sich häufig an Use Cases orientieren. Das SIEM sucht nach bestimmten vorher definierten Angriffsmustern und durchkämmt seine Datenbasis nach entsprechenden Symptomen. Auf diese Weise identifiziert das System bekannte Angriffe präzise und zuverlässig, wertet sie aus und macht sie bspw. über ein Dashboard sichtbar und löst im Idealfall sogar automatisch die geeignete Incident Response aus.
Jedoch ist eine SIEM-Lösung weniger geeignet, um bis dato unbekannte Angriffsszenarien zu erkennen. Denn neue Muster, die noch nicht als Angriffe bewertet wurden, können vom System auch nicht als solche erfasst werden. In der Enterprise-IT kann das SIEM auf umfangreiches Wissen über Angriffspfade zurückgreifen und die hochgradig standardisierte Enterprise-IT-Landschaft ermöglicht ein automatisches, extern zukaufbares Vulnerability-Management. Für das vernetzte Fahrzeug allerdings ist die Ausgangsituation eine andere: Viele

seiner Komponenten sind dediziert für die Fahrzeugplattform entwickelt und angepasst worden, und es gibt kein standardisiert anwendbares oder zukaufbares Vulnerability-Management für diese Komponenten. Alle Erkenntnisse über neue Bedrohungen können also nur aus der Beobachtung der Flotte gewonnen werden, und auch Gegenmaßnahmen müssen zumeist passgenau entwickelt werden.

Vehicle Security Operation Center

Ein Denken in Use-Cases greift hier also zu kurz. Vielmehr benötigt die vernetzte Fahrzeugflotte neben dem technischen Betrieb einer SIEM-Lösung noch einen fachlich-inhaltlichen Betrieb – das Vehicle Security Operations Center (Bild 2). Ein solches Security Operations Center fügt zwei zusätzliche Komponenten in das System ein:

- Eine Threat Intelligence, die Quellen über neue Angriffe und Angriffsmethoden systematisch auswertet und überprüft, ob diese auf die Flotte übertragbar sind. Und die in der Folge „Indicators of Compromise" im eigenen Datenbestand ableitet und gezielt nach Symptomen dieser neuen Angriffstechniken sucht.
- Security-Analysten mit Automotive Security Domänen Know-how, die gezielt nach neuen Bedrohungen suchen und diese in den Logdatenbeständen (Threat Hunting) verfolgen. Dabei dienen ihnen zum Beispiel Erkenntnisse und Auffälligkeiten aus machine-learning-basierten Analysen als Anhaltspunkte bzw. Ausgangshypothesen.

Davon ausgehend können die Security-Analysten potenzielle weitere Schritte im Angriffspfad entdecken und beschreiben (z. B. Lateral Movements) sowie die Analysemethoden des SIEM und der der IDS-Sensoren dahingehend erweitern, dass es Bedrohungsszenarien künftig automatisch erfasst und auf deren evtl. bereits erfolgte Ausnutzung hin prüft. Überdies haben die Security-Analysten die Möglichkeit, die Erkenntnisse aus der Threat Intelligence als Startpunkt für das Threat Hunting zu verwenden, indem sie Informationen aus öffentlich zugänglichen und kommerziellen Quellen hinsichtlich ihrer Relevanz für das Gesamtsystem auswerten.

Alert Validation und verbesserte Bedrohungserkennung

Ein gutes V-SOC sollte dem Flottenbetreiber „actionable information" liefern, also Erkenntnisse über eine bereits eingetretene oder bevorstehende neue Bedrohung, die es ihm erlauben, geeignete Gegenmaßnahmen zu entwickeln, zu testen und auszurollen. In der Regel erfolgt dies über qualifizierte Reports, angereichert durch Evidenzdaten, gepaart mit einer Beratung und Einschätzung der Situation durch qualifizierte Security-Analysten

Dementsprechend besteht eine der größten Herausforderungen und Aufgaben des V-SOC darin, eine Unterscheidung zwischen „falsch-positiven" und „echten" Problemen zu treffen (Alert Validation). Dafür muss für die große Zahl an Assets (klassische ECUs, Domänencontroller, Aktoren, Sensoren u.v.m.), die im Gesamtsystem der vernetzten Fahrzeugflotte vorliegen, ein hoher Grad der Automatisierung angestrebt werden. Zudem müssen für eine situativ effektive und korrekte Bewertung zum Zeitpunkt der Alert-Validation zusätzliche Informationen im V-SOC vorliegen: Wie sind die Softwarestände im Fahrzeuge? Wurden ECUs ausgetauscht? Befindet sich das Fahrzeug in einer Werkstatt?

Das heißt, dem V-SOC müssen Datenquellen des OEMs oder Flottenbetreibers integriert zur Verfügung stehen, um zu verhindern, dass eine Flut falschpositiver Meldungen zu Unbenutzbarkeit oder Alarmermüdung (Alert Fatigue) führt. Letztlich ist die Alert Validation und die Fähigkeit der Security-Analysten, ein machine-learning-basiertes System in der Unterscheidung der Alerts zu trainieren, ein wesentliches Qualitätsmerkmal des V-SOC.

Das Vehicle Security Operations Center reicht damit über den rein technischen Betrieb einer SIEM-Lösung hinaus. Während das SIEM gut geeignet ist, bekannte Angriffe zu erkennen, fügt das V-SOC ihm eine zielführende Infrastruktur und vor allem qualifiziertes Personal hinzu – und ermöglicht so, die Methodik zur Bedrohungserkennung kontinuierlich anzupassen und zu erweitern.

Aufbau weltweit verteilter Security-Strukturen

Für Betreiber großer, mitunter weltweit verteilter Flotten sind Aufbau und Betrieb eines überspannenden Vehicle Security Operations Center eine gewaltige Aufgabe. Um die nötige Zuverlässigkeit und Resilienz zu erreichen, wird es unumgänglich sein, in verschiedenen Regionen weltweit entsprechende Security-Strukturen zu unterhalten. Zudem werden OEMs und große Flottenbetreiber ungeachtet einer Cloud-Infrastruktur allein deshalb schon auf geografisch verteilte Security Operations Center zurückgreifen müssen, um die länderspezifisch unterschiedlichen rechtlichen Anforderungen (bspw. hinsichtlich Datenschutz) zu erfüllen und die angemessene Risikobehandlung ihrer Flotten im Feld gegenüber Genehmigungs- und Aufsichtsbehörden jederzeit nachweisen zu können.

Fazit

Es gibt – für den Bereich der Enterprise-IT – heute bereits leistungsfähige Angebote für verteiltes weltweites Security Monitoring. Auf diese vorhandenen Infrastrukturen und Best Practices lässt sich kosteneffizient zurückgreifen. Zumal sie erwiesenermaßen in der Lage sind, die selbst bei Einsatz eines IDS hohen Datenmengen adäquat zu verarbeiten und Erkenntnisse über neue, zu erwartende Angriffe zu Tage zu fördern. Auf dieser Basis lässt sich ein Zyklus der fortwährenden Beobachtung und gezielten Nachbesserung der Security im Fahrzeug realisieren, der den Vorgaben der neuen Security-Regelwerke entspricht und den Schutzlevel über die gesamte Lebenszeit des Fahrzeugs ermöglicht.. ■ (oe)

www.escrypt.com

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

Dr. Eric Knauel ist Projektmanager Vehicle Security Operations Center bei ESCRYPT am Standort Stuttgart.