



Future Mobility Accelerator

Die Zahl der Cyberattacken auf vernetzte Fahrzeuge nimmt zu. Mit welchen Sicherheitsmaßnahmen können Automobilisten, Zulieferer und Dienstleister darauf reagieren? Und was bedeutet die Einführung der neuen Vorschriften der UN WP.29 für sie?

Einführung

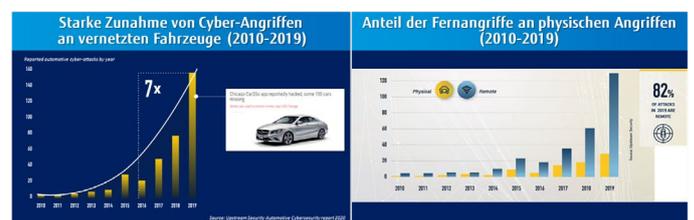
Die Zahl vernetzter Fahrzeuge auf den Straßen steigt. Damit einher geht allerdings auch eine Zunahme der Cyberattacken. Diese Situation macht es notwendig, dass auch die UN Maßnahmen ergreift: Aus diesem Grund hat eine der Arbeitsgruppen, das World Forum for Harmonization of Vehicle Regulations (UN WP.29), neue Regeln in Bezug auf die Cybersicherheit und Software-Updates von Fahrzeugen herausgegeben. Nun ist es an den Automobilherstellern, deren Zulieferern und den kommerziellen Flottenbetreibern, die richtigen Maßnahmen zu ergreifen, um diesen neuen Regeln zu entsprechen.

Steigende Zahl von Angriffen

Die Zahl der Cyberangriffe auf vernetzte Fahrzeuge ist zwischen 2016 und 2019 um das Siebenfache gestiegen. Dabei handelte es sich bei der Mehrheit um Remote-Angriffe über einen bestimmten Netzwerkzugang. Im Jahr 2019 wurden 82 Prozent der Angriffe aus der Ferne durchgeführt. Cyberattacken auf vernetzte Fahrzeuge können über verschiedene Wege erfolgen. Die Top 3 sind

- Server-Attacken,
- schlüssellose Zugangssysteme und
- Smartphone-Apps.

Attackiert werden kann jedes dieser Einfallstore mit verschiedenen Mitteln. Das und die Vielzahl der möglichen Wege, wie Cyberkriminelle ein vernetztes Fahrzeug kompromittieren können, erschwert die Entwicklung passender Sicherheitsmaßnahmen zunehmend.

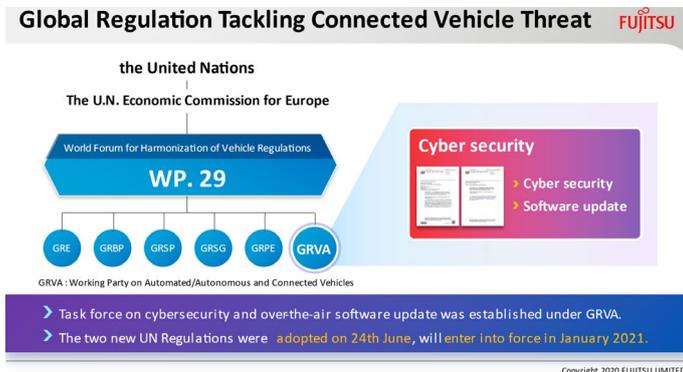


Die Anzahl der Remote-Angriffe übertrifft ständig die der physischen Angriffe
82 % aller gemeldeten Angriffe im Jahr 2019 waren Remote

UN WP.29 hat neue Regeln erlassen

Dies veranlasste auch die Vereinten Nationen (UN), sich mit der Cybersicherheit der neuen Systeme auseinander zu setzen. So wurde das World Forum for Harmonization of Vehicle Regulations (UN WP.29) gegründet, welches die internationale Normierung in Bezug auf Fahrzeugsicherheit und Umweltschutz fördern soll.

Um Sicherheitsthemen für vernetzte Fahrzeuge zu adressieren, hat die UN WP.29 innerhalb ihrer Sektion GRVA zwei Task Forces – „Cybersecurity“ (CS) und „Software-Update“ (SU) – ins Leben gerufen, die am 24. Juni 2020 neue Regeln für CS und SU verabschiedet haben. In Kraft getreten sind die neuen Standards im Januar 2021.



Lebenszyklus-Realisierung des Fahrzeug-Sicherheitsmanagements ist entscheidend

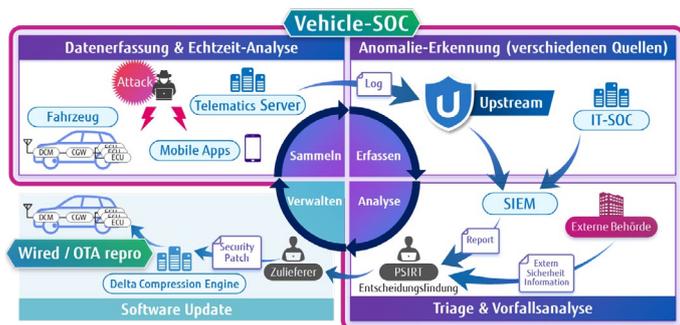
Zulieferer, Geräteproduzenten, Flottenbetreiber und Dienstleister sind ab sofort verpflichtet, die neuen Vorschriften einzuhalten. So ist es im Rahmen des Sicherheitsmanagements notwendig, jedes Fahrzeug durch Erkennung, Analyse und Kontrolle über den gesamten Lebenszyklus aktuell und sicher zu halten sowie vor Cyberangriffen zu schützen.

Daten werden dabei nicht nur von diversen im Auto eingebetteten Sensoren, sondern auch von Telematik-Datenservern oder mobilen Geräten erfasst. Deuten sie auf einen Angriff hin, muss dieser mittels eines SIEM-Systems (Security Information and Event Management) analysiert und das Ergebnis an das PSIRT (Product Security Incident Response Team) gemeldet werden. Dieses entscheidet über die erforderlichen Gegenmaßnahmen, etwa indem es den Hersteller oder Dienstanbieter anweist, Sicherheitspatches, Software-Downloads oder -Updates vorzunehmen.

Auf diese Weise muss der gesamte Zyklus abgedeckt werden – von der Datenerfassung über die Angriffserkennung und Analyse bis hin zur Kontrolle.

Wie man den Zyklus des Fahrzeugsicherheitsmanagements realisiert

Fujitsu unterstützt seine Kunden hier mit zwei Diensten: dem V-SOC Vehicle Security Operation Center for Connected Car sowie dem OTA-Rep programming-System.



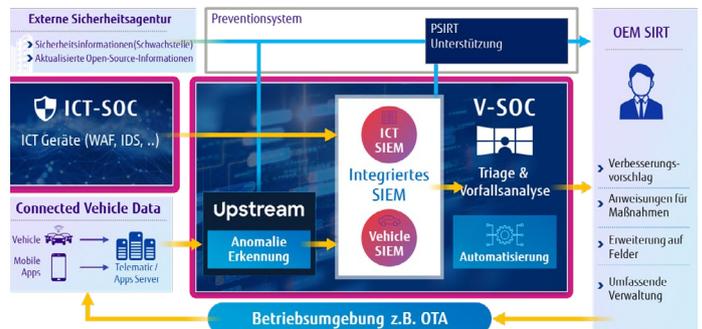
Für den V-SOC Service kooperiert Fujitsu seit Januar 2020 mit Upstream Security, einem Start-up aus Israel mit Fokus auf Sicherheitstechnologie für vernetzte Fahrzeuge.

Mit langjähriger Erfahrung im Bereich ICT-SOC, globaler Reichweite und effektivem Incident-Analyse- und Triage-Service vereint mit Upstreams Cloud-basierter Anomalie-Erkennungs-Engine, neuesten Bedrohungsinformationen sowie AUTOThreat-Know-how bietet Fujitsu einen weltweit wettbewerbsfähigen V-SOC Service.

Gesamtanalyse dank integriertem ICT-SOC und V-SOC

Um ein V-SOC effizient zu betreiben, ist es unerlässlich, nach der Analyse von fahrzeugrelevanten Vorfällen notwendige Gegenmaßnahmen einzuleiten. Aus diesem Grund hat Fujitsu eine Struktur geschaffen, die das V-SOC mit seinem gut etablierten ICT-SOC kombiniert. Auf diese Weise ist es möglich, Vorfälle umfassend zu analysieren. Für unsere Kunden betreiben wir ihre Security Operation Center, überwachen Daten aus verschiedenen Quellen und melden Vorfälle. Für die Analyse und Einordnung der Vorfälle setzen wir auf eine SIEM-Lösung. Darüber hinaus berichten wir regelmäßig über Vorfällen sowie Bedrohungstrends und arbeiten entsprechende Statistiken auf.

Fujitsu verfügt über 17 Jahre Erfahrung im Bereich ICT-SOC und beschäftigt weltweit mehr als 3000 Sicherheitsspezialisten. Mit rund dreizehn rund um die Uhr aktiven Security Operations Centern und 1400 Kunden rund um den Globus gehört Fujitsu im Bereich SOC-Betrieb zu den Weltmarktführern.



Bei den Fujitsu V-SOC-Services verwenden wir die Lösung von Upstream, um fahrzeugbezogene Vorfälle zu erkennen. Diese Vorfälle werden mit diversen ICT-SOC-Vorfällen kombiniert und mithilfe eines SIEM-Systems umfassend analysiert. Anschließend wird das Ergebnis an das PSIRT des Kunden gemeldet. Auf diese Weise sind wir in der Lage, einen umfassenden V-SOC-Service anzubieten, der auch deren Betrieb umfasst.

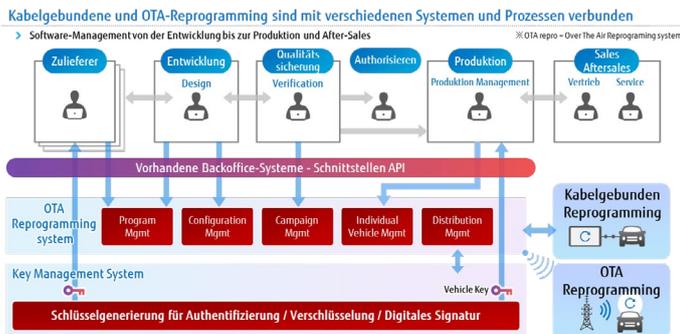
Reprogramming-System, Beratung und Evaluierungstools

Um den Anforderungen der neuen Vorschrift WP.29 SU zu entsprechen, sind neben Prozessänderungen unter anderem auch IT-Systemanpassung sowie die Einführung neuer Fahrzeugentwicklungsprozesse notwendig. Hier kann das Fujitsu OTA-Reprogramming-System helfen: Es ermöglicht Updates ebenso wie den Download von Software – ohne dabei die Funktionsfähigkeit des Fahrzeugs zu beeinträchtigen. Kabelgebunden oder drahtlos über das Mobilfunknetz. So passen unsere Kunden ihre Fahrzeug-IT-Systeme bei Bedarf ebenso schnell wie einfach an. Verfügbar ist auch eine kabelgebundene Reprogramming-Lösung.

Das OTA-Reprogramming-System lässt sich problemlos an verschiedene bestehende Prozesse und Client-Systeme anschließen. Dazu ist das Fujitsu OTA-Reprogramming-System mit einer Reihe von APIs ausgestattet, die eine einfache Integration in bestehende Systeme ermöglicht. Dank der modularen Architektur des Fujitsu OTA-Reprogramming-Systems sind Kunden zudem in der Lage, immer genau diejenigen Funktionen auszuwählen, die gerade benötigt werden oder die ihnen aktuell noch fehlen.

In Zusammenarbeit mit Upstream stellt Fujitsu auf seiner Website ein einfach zu bedienendes WP.29-Evaluierungstool in Japanisch und Englisch zur Verfügung. Mit seiner Hilfe können Kunden ihre bestehenden Sicherheitsrichtlinien validieren sowie eine Sicherheitslückenanalyse durchführen, die auch die Anforderungen der WP.29 CS und SU mit einschließt.

Bei der Einhaltung und Erfüllung der neuen Vorschriften der UN WP.29 unterstützen wir Sie mit unseren V-SOC-Services sowie dem OTA-Reprogramming-System. Für eine sichere Mobilität von morgen entwickeln wir unsere Lösungen und Technologien kontinuierlich weiter.



Über die Bereitstellung von Möglichkeiten zur Anpassung von IT-Systemen über das OTA-Reprogramming-System hinaus bieten wir Automobilherstellern und -zulieferern eine umfassende Beratung und Unterstützung rund um die Einführung der WP.29 SU.

KONTAKT

FUJITSU Technology Solutions GmbH
 Mies-van-der-Rohe-Strasse 8, 80807 München
 E-mail: cic@ts.fujitsu.com
 Website: www.fujitsu.com/de

© Copyright 2021 Fujitsu Technology Solutions GmbH
 Fujitsu und das Fujitsu Logo sind Handelsnamen und/oder eingetragene Warenzeichen von Fujitsu Ltd. in Japan und anderen Ländern. Alle Rechte vorbehalten, insbesondere gewerbliche Schutzrechte. Änderung von technischen Daten, sowie Lieferbarkeit vorbehalten. Haftung oder Garantie für Vollständigkeit, Aktualität und Richtigkeit der angegebenen Daten und Abbildungen ausgeschlossen. Wiedergegebene Bezeichnungen können Marken und/oder Urheberrechte sein, deren Benutzung durch Dritte für eigene Zwecke die Rechte der Inhaber verletzen kann.