Safety in Motion: Cybersecurity for Modern Vehicles

AUTOMOTIVE CYBERSECURITY

As the automotive industry becomes increasingly digital, the risk of cyber attacks on vehicles and their systems is on the rise, making it essential for automakers, suppliers, and other stakeholders to implement comprehensive cybersecurity measures to protect their products and customers.

With more and more vehicles connected to the internet and communicating with other devices, the risk of cyber attacks on vehicles and their systems is increasing. These attacks can take many forms, from theft of personal data to remote hijacking of vehicle controls. The consequences of a successful cyber attack on a vehicle can be severe, ranging from loss of privacy to physical harm. As a result, automakers, suppliers, and other stakeholders must take proactive steps to identify and mitigate potential cyber threats to their products and customers. This requires a comprehensive approach to cyber security that includes not only technical solutions but also policies, procedures, and training. By working together to address the challenges of cyber security in the automotive industry, we can ensure that vehicles remain safe and secure in the digital age.

268 cybersecurity accidents

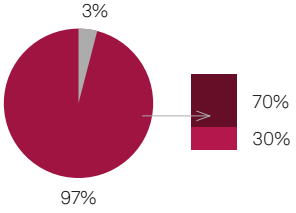
in automotive industry in 2022

+ 25 American OEM EVs remotely controlled by hackers via 3rd party software vulnerability
+ 14 Japanese factories shut down for 24 hours due to cyber attack on supply chain
+ Hackers discovered new attack vector in Chinese OEM vehicle for unapproved software upgrades
+ Years-long phishing campaign targeted German automotive companies for password stealing malware
+ $5 million worth of agriculture vehicles remotely disabled and stolen

97% of all attacks remote

in automotive industry in 2022

+ 3% Physical attacks (e.g. OBD port)
+ 97% Remote attacks, of which
  + 70% long range (e.g., API-based attack)
  + 30% short range: e.g., Bluetooth attack, keyles s entry systems attacks to steal vehicles



New attack types

in automotive industry in 2022

+ 2022 introduced new attack vectors that demonstrate the expansion of cybersecurity threats beyond discrete vehicles, impacting fleets, smart mobility applications and services, EV charging infrastructure, and others
+ EV charging infrastructure accounted 4 % of total incidents
+ API Attacks accounted for 12 % of total incidents

$505 billion

of loss

+ Estimated in the automotive industry due to to cybercrime between 2019-2023

International efforts for an unified approach to protecting against cyber threats

ISO/SAE 21434:2021

Security by design

+ Engineering requirements for each step of product development

UN R155

Cybersecurity Management System

+ Cybersecurity monitoring throughout vehicle lifecycle

UN R155

Threat Analysis & Risk Assessment

+ Risk assessment and risk score for vulnerabilities

UN R156

Software Update Management System

+ Continuous safe updates throughout the vehicle lifecycle

Our Services

Security Consulting

Coordination

+ Handle coordination tasks for cybersecurity, fostering awareness and tackling the challenges of a transforming sector, while preparing for new cyber compliance obligations

Technical consulting

+ Hands-on consulting with given practical experience using the best practices and state of the art in the field

Security Reviews

TARA

+ Cybersecurity risk assessments using best suitable methods to guarantee fullfillness of the company cybersecurity goals

Moderation

+ By techniques to achieve best suitable results and rapid learning curve when executing, for example, a TARA

Secure Product Development

Secure Concept

+ Achieve stunting levels of security, awareness, reaction time by applying state of the art concepts

Secure product requirements

+ By fitting the security scope into product operating environment and regulatory expectations

Security Test Suite

Security test plans

+ Development of test plan strategies to achieve target cybersecurity goals

Security test specifications

+ Best practice security test specification techniques to support the proper verification goals

Penetration Testing

Vulnerability Scanning

+ By using a dedicated penetration test laboratory and finding the efficient dosis of needed effort to meat todays security demands

Fuzzing (CAN, Ethernet)

+ By scan your interfaces or APIs for unexpected behavior

Trainings

Certified Cybersecurity Engineer & Manager

+ By in house trainings or by training provider TÜV Austria

Customised

+ Support your teams to meet regulatory cybersecurity demands (eg UNECE WP29, Methods, ...)

Compliance Planing

UN R155 - CSMS

+ We walk through with you to meet the requlatory expectations for each variant: as OEM, TierX-Supplier or Service-provider

UN R156 - SUMS

+ Also by choosing the best suitable variant management system for your environment

Others

Certification planning

Internal audits

Secure code analysis

Secure coding guidelines

Technical reviews

Would you like to learn more about our offerings? We look forward to hearing from you.

Borislav Nikolov

Head of Cyber Security I Mobilily Solulions

+43 664 6276805
borislav.nikolov@msg-plaut.com

msg-plaut.com/at

msg Plaut Austria GmbH

Modecenterstraße 17/4/6 | 1110 Wien

msg-plaut.com
office.at@msg-plaut.com

Best of Both

.msg PLAUT