Cybersecurity for the automotive industry

Driving digital – securely

Security in the automotive industry raises several distinct challenges around the connected vehicle, as well as in manufacturing plants and across enterprise IT systems. These challenges appear at each stage of the plan-build-run lifecycle. Capgemini offers an end-to-end approach with comprehensive services to help companies ensure every base is covered.

Why cybersecurity is now a hot topic

Until two or three years ago, automotive companies tended to see the security of vehicles, manufacturing plants, and enterprise IT systems as pretty much independent. "Security by obscurity" was a widely used paradigm. With most companies keen to hush up security breaches, it was an easy issue to ignore.

Security has recently come to prominence for several reasons. The car is now an intelligent, communicating device, with hundreds of intelligent, communicating parts – which add up to a large attack surface. Hacks into cars have attracted a lot of media and public attention; according to one survey, 62% of customers fear cars will be easily hacked.[1]

1 Kelley Blue Book, In-Vehicle Technology Survey, August 2015, reported in RSA Conference 2016 presentation, "Braking the Connected Car: The Future of Vehicle Vulnerabilities" https://www.rsaconference.com/writable/presentations/file_upload/ht-t11-hacking-the-connected-car-thetfuturetof-vehicle-vulnerabilities.pdf

It's not only the security of the vehicle itself that is attracting attention. The security of manufacturing plants is also a growing concern. A recent report on worldwide security breaches stated that "automotive manufacturers were the top targeted manufacturing sub-industry, accounting for almost 30 percent of the total attacks against the manufacturing industry in 2015."[2]

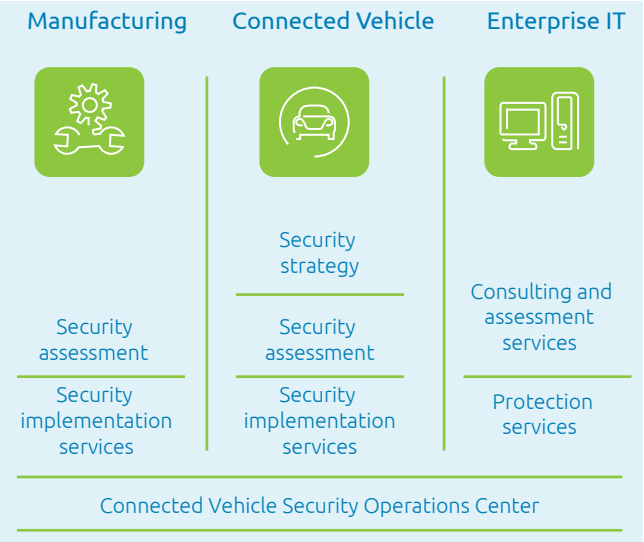
As a result, CEOs in large automotive companies are now taking a strong interest in security, and are constantly asking their reports what their strategy is and how safe the company is. Automotive manufacturers are keenly aware of the need to secure vehicles, and to reassure customers who have read media reports suggesting they are not secure.

Achieving the required level of security is often far from straightforward, particularly when it's necessary to safeguard legacy components that were not designed to be connected to the internet. Capgemini has a comprehensive range of cybersecurity services to help the automotive industry overcome this challenge.

Introducing Capgemini's cybersecurity services for automotive clients

Capgemini takes an end-to-end approach to their customer's cybersecurity. Our services have three focus areas that together cover the complete ecosystem: manufacturing, connected vehicle, and enterprise IT. The services span the entire product lifecycle including the plan and build phase and the run phase.

Capgemini's comprehensive cybersecurity services for the automotive industry



2 IBM X-Force® Research 2016, Cyber Security Intelligence Index, "Reviewing a year of serious data breaches, major attacks and new vulnerabilities: Analysis of cyber attack and incident data from IBM's worldwide security services operations". P7 http://www-03.ibm.com/security/data-breach/cyber-security-index.html

Our services to support end-to-end security are built around the Defense-In-Depth paradigm. This ensures that security is built in at every level during plan and build, and maintained during run.

As shown in the diagram, our services can be viewed in two dimensions, and we have offers at each intersection. For plan and build, our offers include strategy, assessment, and implementation. For run, our offer focuses on the Security Operations Center (SOC).

Capgemini's offers for the plan and build phase

During plan and build, our offers address the three focus areas shown in the diagram: connected vehicle, manufacturing, and enterprise IT. We build in proactive measures from the start so that security is an integral part of the deliverable.

The connected vehicle

Vehicles on the road are vulnerable to hacking, both of the vehicles themselves and of the back-end IT systems to which they connect; both must be secure.

This challenge is increasingly important because of the growing computing power of vehicles. We are only at the start of this process. In the future, there will be many more vehicle-to-vehicle and vehicle-to-hub communications. There are already plenty of discussions about these ideas in the media, arousing concern among consumers. The idea that you could be driving along in the outside lane of a motorway when someone takes over your car is not pleasant.

Areas where Capgemini can help include:

- Designing a **strategy** to secure every aspect of the vehicle from ECUs, buses and external connectivity to the governance processes around each of them. Such a strategy enables a manufacturer and its suppliers to create end-to-end security. However, putting this strategy in place is complex; it requires a deep understanding of the vehicle and its parts as well as the ability to turn the strategy from concept to reality across multiple departments and organizations.
- **Assessment** of security within and around the car. Experts can review the strategy for securing in-vehicle elements such as ECUs and sensors and the buses that connect them. The assessment's scope may include the security of external connections, for example via Wi-Fi or Bluetooth, to the carrier and then to the back end or a service provider such as Google. The team can then recommend remedial actions. Assessment can include penetration testing ("pentesting") to provide additional insight into vulnerabilities.

- **Implementation** of security measures and remedial actions. This includes consulting and training on secure software development good practice, and operational implementation in the software development lifecycle. Once again, pentesting can be used to check that implementation has been successful.

We offer a range of services to help secure the connected vehicle back end as well as the vehicle itself. The connected vehicle back end is often treated as part of enterprise IT, and is discussed below.

The manufacturing plant

Hackers can attack a manufacturing plant that assembles cars or produces parts for cars. The increased tendency for manufacturing systems to be connected to enterprise systems and the internet – for example, for remote maintenance and management – creates more opportunities for attack. Legacy hardware and software that were not designed for the internet are particularly vulnerable.

> "In Fiscal Year (FY) 2015, 295 incidents were reported to ICS-CERT, and many more went unreported or undetected. The capabilities of our adversaries have been demonstrated and cyber incidents are increasing in frequency and complexity." Report from FBI and DHS based on ICS-CERT[3]

Attacks come from anywhere in the world and from a wide range of adversaries including terrorists and nation states bent on sabotage. With the manufacturing plant made up of intelligent, connected machines, a hacker can target any point and then reach other points in the plant. These attacks can cause huge damage.

Services that Capgemini offers to help with manufacturing plant challenges include:

- Organizational and architectural maturity **assessment** to provide global positioning of the level of risk, and to highlight the critical subsystems for which deeper risk analysis is needed. The assessment generates mitigation recommendations and next steps for the future (e.g., priorities, budget, make or buy, gap analysis with legal constraints).
- **Implementation** includes remedial action, potentially with further pentesting.

Enterprise IT

The security of enterprise IT systems and the protection of personally identifiable information (PII) are as vital for automotive companies as for any other organization – after all, in addition to industry-specific solutions, they have the same general solutions in back-office areas like finance and HR, and all the vulnerabilities that come with them.

As well as those common risks, automotive companies have the additional ones that arise from connecting to vehicles and manufacturing systems. They must also operate back-end systems to carry out services required by connected vehicles. For example, when a driver requests a map service, a back-end system may need to check that they have permission to use the service and then route the service to the vehicle.

In this example, the map service itself, and possibly also the checking and routing, may be outsourced. Some companies outsource enterprise IT extensively. Any form of outsourcing adds an additional dimension to the security challenge, and so does hosting services in the cloud.

Once again, given today's levels of connectivity, a hacker who penetrates general IT systems can probably use them as a platform to access the manufacturing operation, and maybe the vehicle itself. Enterprise IT systems are also especially vulnerable to insider attacks.

Capgemini has deep experience securing enterprise IT. We can help you safeguard your enterprise IT against cyber-attacks and internal malicious behavior with end-to-end advisory, protection, and security monitoring services. Our services are described here.[4]

Capgemini's offers for the run phase

However thorough the plan and build phase is, inevitably some security issues will not be caught. Therefore, we help you react, with predefined responses to any given type of attack.

The **SOC (Security Operations Center)** is key to our offers for the run phase. It can act as mission control, looking for anomalous behavior in any aspect of the operation, and tracks events, incidents, and responses. It integrates well with existing service management organizations and procedures. With the vehicle as the focus, the SOC can look for unexpected occurrences such as a vehicle being unlocked or started in an unusual way or at an unusual time. The SOC can process alerts and raise incidents based on them; it does not intervene in real-time, however. It's not just about the vehicle; a full-blown SOC spans connected vehicle, manufacturing, and enterprise IT. In fact, enterprise IT is usually the starting point.

3 US Department of Homeland Security, "Seven Steps to Effectively Defend Industrial Control Systems https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf https://www.capgemini.com/cyber-security-services

4 https://www.capgemini.com/cyber-security-services-and-solutions

Why work with Capgemini on cybersecurity?

At Capgemini, we encourage our clients to view cybersecurity in the context of their business transformation goals, and to treat security as a business enabler rather than a problem.

Our cybersecurity team combines security expertise with deep knowledge of the automotive industry and of manufacturing. This means Capgemini can think strategically and then implement its recommendations. The cybersecurity team is used to working with engineers and can explain security concepts in business terms rather than IT jargon.

We have an exceptionally strong background in securing enterprise IT systems. We have worked in this area for many years with some of the world's most security-conscious organizations from sectors like financial services, government, nuclear energy, and aviation.

We operate eight SOCs worldwide and have the data science expertise to help clients ensure that they can identify incidents and respond rapidly and appropriately. We also help clients progressively automate this work.

Our many recent security success stories from the automotive industry include the following:

- We reduced the attack surface of a major tier 1 supplier by defining and implementing a standard security architecture applicable to all manufacturing sites worldwide.
- We helped a global OEM develop a consistent and predictable approach to connected vehicle security for use by both internal functions and suppliers. The approach reflects industry standards and relevant guidelines for secure software development.
- We are detecting security incidents for a global OEM across the whole IT landscape including vehicles and manufacturing plants. We are working on extending the service to this client's entire product range.

For more details contact

Dr. Magnus Gerisch
Application Technologies, Automotive
magnus.gerisch@capgemini.com

Nick Gill
Chairman, Automotive Council
nick.gill@capgemini.com

Jérôme Desbonnet
Sogeti, Global Cybersecurity CTO
jerome.desbonnet@sogeti.com

About Capgemini and Sogeti

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of 200,000 team members in over 40 countries. The Group reported 2017 global revenues of EUR 12.8 billion.

With 3,000+ cybersecurity experts, Capgemini and Sogeti offer a full range of services that safeguard the digital and cloud platforms, IT infrastructures, and OT systems of companies and administrations worldwide. Our security specialists use the very best technology products tested and proven by our own R&D team specializing in malware analysis and forensics. We have ethical hackers, an international network of multi-client security operation centers (SOCs) and are global leaders in testing. We Advise. We Protect. We Monitor.

For more information visit:
www.capgemini.com or www.sogeti.com

About Capgemini's Cybersecurity Practice

Capgemini and Sogeti are experts in IT infrastructure and application integration. Together, we offer a complete range of cybersecurity services to guide and secure the digital transformation of companies and administrations. Our 3,000 professional employees support you in defining and implementing your cybersecurity strategies. We protect your IT, industrial systems, and the Internet of Things (IoT) products and systems. We have the resources to strengthen your defenses, optimize your investments and control your risks. They include our security experts (Infrastructures, Applications, Endpoints, Identity and Access Management), and our R&D team that specializes in malware analysis and forensics. We have ethical hackers, eight security operations centers (SOC) around the world, a Information Technology Security Evaluation Facility, and we are a global leader in the field of testing.

For more information:
www.capgemini.com/cybersecurity

About Capgemini's Automotive Practice

Capgemini's Automotive practice works with most of the leading automotive companies in the world. More than 7,500 specialists generate value for our clients every day through global delivery capabilities and industry-specific service offerings across the value chain, with a particular focus on our AutomotiveConnect propositions for OEMs, suppliers and retailers.

For more information:
www.capgemini.com/automotive