Fortifying automotive supply chain security

By Andre Froneman, Senior Technical Specialist at Datacentrix

As connected vehicles become increasingly prevalent, the automotive industry faces unprecedented cybersecurity challenges. To understand the damage that can be wrought by cybercriminals, we need only look at examples of supply chain attacks over recent years, including automotive component suppliers, a global automotive logistics and shipping company, and even a South African rail, port and pipeline company.

In response, the United Nations Regulation No. 155 (UN R155) has been established to set a global cybersecurity standard for the entire automotive value chain, extending beyond the vehicle itself. It mandates comprehensive security practices across development, manufacturing and distribution, requiring all stakeholders to uphold stringent protection measures.

Key focus areas under UN R155 include:

- **Supply chain security:** Protecting against vulnerabilities introduced by third-party suppliers and partners through remote access to software, programmable logic controllers (PLCs), robots, controllers, monitoring devices and more.
- **Data privacy:** Ensuring the confidentiality, integrity and availability of sensitive vehicle data shared, from component suppliers all the way through to dealerships and customers.
- **Incident response:** Developing effective plans to detect, contain and mitigate cybersecurity incidents that are managed in accordance with the Trusted Information Security Assessment Exchange (TISAX), an assessment and exchange mechanism for information security in the automotive industry, UN R155, and IEC 62443 cybersecurity best practice controls and frameworks.

> The United Nations Regulation No. 155 (UN R155) has been established to set a global cybersecurity standard for the entire automotive value chain, extending beyond the vehicle itself. It mandates comprehensive security practices across development, manufacturing and distribution, requiring all stakeholders to uphold stringent protection measures.

- **Continuous monitoring:** Implementing ongoing security assessments and threat intelligence on information technology (IT) and operational technology (OT) systems.

Attacks from all angles

Attacks within the auto supply chain space can originate from multiple angles. These could include electrical distribution, generation and transmission; water or gas supplies; component suppliers; port, harbour or rail disruptions; logistics operation companies working inside the factory; or shop floor programmable logic controller (PLC) equipment OEM breaches.

Using non-secured component suppliers can result in several risky, complex scenarios. For instance, with geopolitical tensions on the rise, manufacturing is disproportionally affected by 'accidental'

> To strengthen cybersecurity and comply with TISAX and UNECE standards, South African automotive organisations should begin with a comprehensive risk assessment to pinpoint vulnerabilities. Datacentrix recommends adopting advanced cybersecurity technologies for OT, procurement and dealership protection, alongside regular workforce training, including non-IT employees, on security best practices.

ransomware that is deployed from IT or contractors' laptops, USBs or internet access. Here, a supplier's IT systems could be compromised by a ransomware attack, encrypting their data and demanding a ransom payment. The result is that the supplier's operations are disrupted, leading to delays in component delivery, potential data breaches, and financial losses.

Another conceivable scenario is that of a supply chain phishing attack, where phishing emails are sent to employees at various levels of the supply chain, targeting sensitive information like login credentials or financial data. Compromised credentials could be used to gain unauthorised access to systems, disrupt operations, or steal valuable data.

Additionally, botnet-enabled distributed denial-of-service (DDoS) attacks, which are used to launch attacks on suppliers' websites or IT infrastructure, should be of concern. The impact of this type of incident is that attacks can not only overwhelm systems and disrupt operations but also cause incredible reputational damage.

Another possible situation could be the targeting of suppliers to steal sensitive intellectual property related to vehicle design, manufacturing processes or software, which can lead to competitive disadvantages, financial losses and even legal consequences. By the same token, stolen sensitive customer data, such as personal information or financial details, can result in identity theft, financial fraud and damage to the supplier's and manufacturer's reputations.

Industrial espionage is another significant danger – cybercriminals could target suppliers to gain access to confidential information about vehicle development, manufacturing processes or supply chain vulnerabilities, which can then be used to gain competitive advantage, disrupt operations, or even be sold on the black market.

Finally, it's critical to take measures to protect against supply chain malware attacks. Under these circumstances, malware could be introduced into the supply chain through compromised components or software, targeting vehicle systems or manufacturing equipment, thereby disrupting operations, compromising vehicle security, and leading to potential safety risks.

What can local automotive organisations do to increase protection?

To strengthen cybersecurity and comply with TISAX and UNECE standards, South African automotive organisations should begin with a comprehensive risk assessment to pinpoint vulnerabilities. Datacentrix recommends adopting advanced cybersecurity technologies for OT, procurement and dealership protection, alongside regular workforce training, including non-IT employees, on security best practices.

It's also possible to perform offline cyber audits for new equipment, where shop floor equipment can be scanned at staging or pre-production planning and certified as virus, malware and configuration risk free at that time and place.

Furthermore, PLC code protection offers advanced PLC versioning, code management, code backup and function block level deployment services. This removes IP from engineering workstations and puts code in secure locations that are easily backed up, restored and documented for compliance and audits.

South Africa has an excellent automotive heritage, but there is still much work to be done to protect these businesses. As a hybrid ICT systems integrator and managed services provider, Datacentrix believes it is our duty to help support companies within the supply chain and ensure that they are better tooled and supported in their fight against cyber-attacks.

For more information contact Elzette du Preez on edupreez@datacentrix.co.za