OT Cybersecurity insights to mitigate the risks effectively

A complete overview of vulnerabilities helped Jacobs Douwe Egberts (JDE) to mitigate risks by implementing adequate mitigation measures. CGI proved to be a reliable partner in OT / ICS security, adding value and improve factory cyber security posture and decrease risks.

JDE is part of JDE Peet's, the world's largest pure-play coffee and tea company, headquartered in The Netherlands, with a strong portfolio of global, regional and local brands.

In 2017 one of the brands was impacted by a malware incident that caused a computer outage across global operations and disrupted shipping and invoicing during several days, resulting in a €100M loss. This was a major trigger to start a cybersecurity program across entire Operational Technology (OT) / ICS environment in all factories.

The Challenge

It is no much of a secret that the manufacturing industry is one of the most targeted industries when it comes to cyberattacks. There's often no sufficient expert knowledge and capacity to address cybersecurity threats effectively. JDE needed expert insights and the overview of all cybersecurity risks and mitigation of all threats and vulnerabilities in its factories. This included all operational technology computing systems that are used to manage the entire industrial operation.

The solution

To assess the OT / ICS environments in JDE factories, CGI used its OT Security Assessment. This approach provides insights into the maturity of the OT security policy in place and the way in which this policy has been implemented. This approach includes well-prepared site visits, structured interviews with key employees, examination of the factory against the IEC62443 standard and an OT / ICS network topology scan.

Specialized equipment is connected to the OT / ICS network to do an automated asset discovery and generate a topology map that shows all relevant assets in the OT / ICS environment and way they are all interconnected. Data traffic from the plant supervisory, direct control and field level are checked on specific cybercrime-sensitive areas.

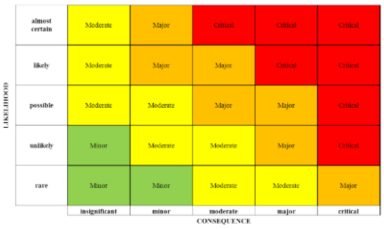
An OT / ICS Cyber Security Assessment typically includes:

- Maturity assessment
- IEC62443 / NIST800 assessment
- In-factory validation phase
- In-factory discovery phase, examining both the physical and logical OT / ICS security and documented findings
- OT / ICS network scan and analysis, including asset discovery, anti-malware landscape, identity & access mgt., firewalls and remote access

CGI OT security assessments are based on relevant worldwide ICS compliancy standards like NIST and ISO/ISA/IEC.

CGI executed these assessments with multiple on-site assessor teams (each consisting of two assessors) specialized in OT security, using uniform approach for consistent reporting. Assessment preparation, firewall and network analysis as well as OT / ICS architecture evaluation was provided from CGI OT Security Centre of Excellence, centrally.

A risk inventory and risk heat map, mitigation advice and budget indication for every specific mitigation advice was included in the assessment report as requested by JDE.



LIKELIHOOD	insignificant	minor	moderate	major	critical
almost certain	Moderate	Major	Critical	Critical	Critical
likely	Moderate	Major	Major	Critical	Critical
possible	Moderate	Moderate	Major	Major	Critical
unlikely	Minor	Moderate	Moderate	Major	Critical
rare	Minor	Minor	Moderate	Moderate	Major

CONSEQUENCE

The risk assessment, covering risks, likelihood and impact, advised mitigations were pre-prioritized and helped JDE to define its OT / ICS cybersecurity priorities moving forward.

Raising awareness

Following the assessments and report out an OT / ICS cybersecurity awareness video has been created, based on the findings from the on-site assessments. This video is distributed to JDE factory workers for OT / ICS cybersecurity training purpose.

Why CGI?

JDE selected CGI for its capability in mission critical environments and OT cybersecurity expertise with the capacity and ability to assess all of JDE's factories worldwide, with a uniform approach and within the time frame set out. CGI provided large enough team of specialists with deep knowledge in the process control domain. Following the assessments, CGI was tasked by JDE to implement relevant mitigation measures. By improving cybersecurity posture of JDE factories CGI proved to be a reliable partner in OT / ICS security.

About CGI in Cybersecurity

CGI has a 40 year heritage of creating and securing critical business systems in complex and mission critical environments worldwide, including defense and intelligence sectors.

We have invested heavily in establishing our credentials, working closely with international security associations and standards bodies. While cyber threats are global, we know that requirements vary locally and challenges are unique to each organization. Through our expert talent, deep technical and business knowledge, security operations centers, best practices and frameworks, we work to ensure controls are baked in, not bolted on.

About CGI

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world. Operating in hundreds of locations across the globe, CGI delivers end-to-end services and solutions, including strategic IT and business consulting, systems integration, intellectual property, and managed IT and business process services.

For more information

Visit cginederland.nl
Email us at info.nl@cgi.com