How the Cyber Security challenges increase due to Industry 4.0

The fourth industrial revolution, or Industry 4.0, is seen as the next step after the computer automated industrialisation that happened during the last five decades. This new revolution is powered by buzzwords like IIoT – (Industrial Internet of Things) big-data and A.I.

No matter how a chemical facility is made "smarter", all these technologies have two things in common, it is all driven by data, and it requires hyperconnectivity. And this is the next challenge for Cyber Security within industrial environments.

Background

The reason for Industry 4.0 is clear. The drive within the chemical sector to improve is crucial. Moreover, the chemical industry also contributes to almost any other manufacturing supply chain so there is also lot of potential. Product improvement, cost efficiency, business optimisations are some of the drivers for this digital transformation. All the more reasons to expect this trend will continue. But again, what about Cyber Security?

Challenges the Industry 4.0 initiatives pushes forward to hyper connectivity, which results in more exposure of OT networks, usage of more generic IT services, cloud connectivity and "bypasses" the traditional segmented models. This isn't necessarily a bad thing if Cyber Security is not an afterthought.

Challenges explained

It is not always obvious that IIoT devices create new Cyber Security challenges as at first glance they often seem perfectly protected. Many IIoT vendors recognise the need of Cyber Security and deliver more secure and more capable devices. However, when poorly implemented or improperly maintained they can still introduce an unknown risk. Therefore, these cyber risks could be generally divided in two types, the IIoT solution itself and the implementation of the solution.

Solution

Most important is to immediately incorporate Cyber Security during the design process of these new solutions, especially when IIoT or other remote connectivity is involved. This is not only applicable for new facilities but also for expansions or modifications.

The OT network is not always suited to incorporate all technical requirements and at the same time the technical expertise might be lacking. Moreover, as most of these solutions are business or operations driven, they might overlook the Cyber Security implications during the project phase altogether.

Finally, many IIoT implementations require "connectivity" that may already exist in a facility or are sometimes unknown to the end-user.

Conclusion and the way forward

It is expected that the Industry 4.0 and IIoT trend will continue for all sectors, including the Chemical sector. This will be primarily driven by the business and operational benefits. This is a fine so long as Cyber Security is not an afterthought. It's important to include security design and operational costs directly into the business case of these smart initiatives and verify their impact on the OT Cyber Security posture. Internal and external security design reviews could assist in this stage. For existing solutions and systems there are multiple approaches: eg

- to review

- verify the current security state

- proactively solve potential issues before they create any business impact

The end goal remains to achieve safe, reliable, and cost-effective production and to manage cyber risk to an acceptable level to support those goals.

Bureau Veritas is able to support with strategy with regards to cyber security compliance and maintenance.-

- Analysis and recommendations on how to improve security
- Testing to ensure possible vulnerabilities are found and addressed
- Assisting to implement processes and procedures so that Cybersecurity becomes an every day habit
- Helping staff to become part of the security solutions

For further information visit - https://www.bureauveritas.co.uk/