EVOLUTION OF CYBER SECURITY WITHIN TANK TERMINALS

Ensuring a safe work environment has been at the forefront of tank terminal organisations since the beginning. Companies implemented safety measures across their organisations. Health, safety and environment (HSE) has become an integral part of tank terminal operations. The introduction of automation allowed tank terminals to improve their (primary) processes, making them more efficient and safer. However, this increases the risk of cyber incidents that can impact HSE.

Cyber security risks for tank terminals are present in all forms. Threats can originate from inside and outside the organisation and are continuously evolving. This means that cyber security resilience needs to evolve as well. Tank terminal operations must be prepared by being aware of the latest threats and they must know what to do in case of a cyber-attack. It is recommended that cyber security is well integrated in the operation of any tank terminal. Only if this is the case can tank terminals ensure that cyber risks are managed appropriately.

HISTORY

In the past, cyber security was not considered in many of the installations. In case cyber security was considered, it was mainly focused on the information technology (IT) or office automation side of the business. The operational technology (OT) or process automation side was deemed not vulnerable since it was considered independent of IT and was not directly connected to the outside world. Interaction between OT and IT was often limited to support by IT-personnel of the computers that were used for word-processing, calculations, email and fixing broken printers.

The focus was mainly on IT-related technical solutions, like antivirus software, that were implemented ad-hoc and were not considered part of a managed effort towards integrating cyber security within the organisation. This changed for OT when more mainstream servers were used to host operational technology related applications. Where previously most systems were proprietary or based on a version of the UNIX operating system, Microsoft Windows systems became the operating system of choice. This was mainly because it became cheaper to develop applications for these servers and easier to provide support.

As the industry became used to up-to-date information from their financial and other IT-systems, the industry saw the advantages of using up-to-date process information in office automation applications like ERP, it became a business need to communicate with the OT-systems. This meant that IT-security settings or configurations, like controlling access using a domain controller or the introduction of antivirus solutions, became more common within the OT-environment.

This created an area of tension between OT- and IT-personnel due to the difference in focus. The OT-systems were originally built around an infrastructure that focused on HSE and maintaining the primary process. IT would be frequently asked for advice, since they had experience with the new systems, without fully understanding the focus of OT-personnel on HSE and the continuation of the primary process. As a result, IT often tried to implement IT related security measures in an OT-environment, both technical and organisational, without considering the differences between the two environments. Hudson Cybertec often encounters this in companies where a shared physical infrastructure is used for OT and IT.

CURRENT SITUATION

This resulted in the current situation where most tank terminals have a legacy infrastructure that was designed without considering cyber security as compared to what is accepted within the industry today. New installations or projects that intend to upgrade the current infrastructure need to take this into account, both to ensure that these do not pose a (cyber security) risk to the legacy infrastructure or vice versa. Larger organisations with multiple locations and terminals often have tank terminals with different infrastructures and levels of automation, ranging from tank terminals with manual operation or limited automation to highly automated tank terminals.

Hudson Cybertec, as an independent provider of cyber security consultancy and services for operational technology, often encounters tank terminals that struggle with the implementation of cyber security within their own organisation. One of the reasons that tank terminals struggle is because most do not have an up-to-date overview of their own infrastructure, both for their IT- and OT-environments. The situation is even more complex in larger organisations that have multiple terminals, how can they ensure that current cyber security risks are properly managed, mitigating the risk that cyber security incidents pose to the organisation?

OUTLOOK

Cyber security is a hot topic, daily news articles regarding security incidents are making headlines around the world. The threat landscape is evolving, especially the shift towards more targeted attacks where attacks focus on specific people, systems or organisations; CEO fraud where money is fraudulently obtained; storage spoofing where fake websites are created and then used for fraudulent business and the increasing focus on industrial automation and control systems. Since the threat landscape is constantly changing, companies need to ensure that their organisations and their infrastructure is resilient to cyber security incidents.

As more emphasis is given to mitigating cyber security risks, in part due to due diligence requests from insurers, stakeholders and regulation, tank terminals should manage cyber security in a controlled manner within their organisation. Often tank terminals do not have the resources or relevant expertise to ensure that cyber security becomes part of doing business. Support from outside the organisation is often necessary in these situations. Most cyber security support is focused on cyber security for IT-solutions and often does not consider OT. Hudson Cybertec's internationally recognised industry expertise is relied on by tank terminals to help them integrate cyber security within their organisations.

MANAGE CYBER SECURITY

To manage cyber security, industry derived cyber security standards are frequently used as a basis. For example, the IT-environment can use a cyber security standards framework like the ISO 27k series while the OT-environment can use the cyber security standard IEC 62443 for Industrial Automation and Control Systems. The IEC 62443 standard specifically provides guidance, based upon industry best practices, to manage cyber security within an OT-environment using a cyber security management system (CSMS). These cyber security standards consider security measures which address the three areas of cyber security: people, process and technology.

Tank terminals that have already considered cyber security in the IT-domain can choose to incorporate cyber security for the OT-domain rather than reinventing the wheel. As such, cyber security should be considered as part of existing processes, HSE measures, policies and procedures.

A CSMS as specified in the IEC 62443 should be aligned with the organisation's vision and goals. An effective implementation determines the right balance of security measures that address people, process and technology. IEC 62443 addresses each of these, for example: training and awareness addresses people, policies and procedures address the process and system requirements address technology. Hudson Cybertec has a thorough experience supporting companies with the development and implementation of a CSMS which is tailored to each organisation's specific cyber security requirements.

KNOW YOUR INFRASTRUCTURE

Decisions on how to implement cyber security within a tank terminal can only be made if the company knows where it stands with regard to cyber security. Organisations often overestimate their own cyber resilience level since most of their cyber security measures are taken in the IT-domain. Cyber security measures taken in the OT-domain are often only of a technical nature. As such, there is often a gap between the current and the desired situation.

Therefore, as the first step to take control of cyber security, Hudson Cybertec often performs a baseline measurement in form of a cyber security assessment as a starting point to improve cyber security at a tank terminal. This gives the organisation a clear overview of its challenges in the area of cyber security. It also allows the company to define and focus on those aspects of cyber security that have the highest priority for the organisation or need to be remediated first. In addition, it allows the tank terminal to identify so called 'quick wins' that can be easily implemented without too much effort.

FOR MORE INFORMATION

This article was written by Ilya Tillekens, senior consultant at Hudson Cybertec, a cyber security consultancy & services provider for operational technology, with full emphasis on critical infrastructure including the tank terminal sector.

www.hudsoncybertec.com/en/tsm