ORGANISING CYBER SECURITY IN TANK TERMINALS

The European Union introduced legislation (the NIS directive) that became active on November 9, 2018. The goal of the Network and Information Security (NIS) directive 2016/1148 is to boost the overall security in the EU, with a focus on increasing the security level of organisations involved in critical infrastructure.

Marcel Jutte, managing director of Hudson Cybertec, says: 'Industries like tank terminals often do not have an adequate cyber security organisation in place to protect the terminal against attacks.

'In case of a successful breach, this is often not detected and as such networks are compromised and intruders are present on their networks. We often encounter situations where organisations overestimate their cyber security resilience. Reliance on existing security measures for safety instrumented systems (SIS), the usage of outdated policies and procedures all give a false sense of security.

'Action is only taken when forced by external factors like legislation, as an insurance requirement or an incident to a facility or a facility of a competitor.'

EU NIS DIRECTIVE 2016/1148

Based on the NIS directive 2016/1148, each EU member state has introduced local legislation that implements the directive into local law. For example, in The Netherlands this is done by the 'Wbni'. Part of the legislation is a 'duty of care', this implies that organisations that must adhere to the legislation, must implement cyber security measures within their organisation.

Jutte: 'The international cyber security standard IEC 62443 can provide the framework to implement cyber security within the Industrial Automation and Control Systems (IACS) domain. The IEC 62443 is based upon the ISO 27000 series and considers all the specific cyber security requirements for an IACS environment with emphasis on preventing cyber incidents that have health, safety & environment (HSE) implications.'

TAKING CONTROL OF CYBER SECURITY WITH THE IEC 62443

Jutte: 'To take control of your cyber security, the IEC 62443 provides the structure for a tank terminal. Within the IEC 62443, the standard IEC 62443 2-1 provides the framework for the development and implementation of a Cyber Security Management System (CSMS) in order to integrate cyber security within a tank terminal organisation.

'Hudson Cybertec has thorough experience supporting organisations with the development and implementation of a CSMS. The management system is tailored to each organisation's specific requirements.'

PEOPLE, PROCESS, TECHNOLOGY

A CSMS as specified in the IEC 62443 takes into account the three pillars of cyber security: people, process and technology and should be aligned with the organisation's vision and goals. An effective implementation is determining the right balance of security measures that address people, process and technology. The IEC 62443 addresses each of these.

IMPLEMENTING A CYBER SECURITY MANAGEMENT SYSTEM

'In order to implement a CSMS it is important to know where the organisation stands at this moment regarding cyber security,' explains Jutte.

'Therefore, we advise to start with a zero-measurement security assessment. This gives the organisation a clear view of what its weaknesses are and allows it to define and focus on those aspects of cyber security that need to be remediated first. In addition, it allows the organisation to identify so called 'quick wins' that can be easily implemented without too much effort.'

IEC 62443

'The IEC 62443 2-1 provides guidance for the development and implementation of a CSMS. For most organisations, it is not feasible to develop and implement a CSMS in one go. Therefore, tank terminals should focus on those elements that are the most important to the organisation and this is different for each company.'

ROLLING START

Not all tank terminal companies have the knowledge, experience and resources on hand to facilitate a thorough and structured development and implementation of a CSMS using the IEC 62443.

'The development and implementation of a CSMS can take several years depending on different factors,' says Jutte.

'Such an implementation requires a structured approach. To ensure the success of the development and implementation of the CSMS, organisations often ask Hudson Cybertec for help. We provide everything from ad-hoc support to an organization on one end to a full-service package where we provide a COSO who will manage the development and implementation of a CSMS.

'We currently have several CSMS projects at tank terminals where we provide these services. In order to ensure a rolling start of a project, we provide additional resources at the start of the project to ensure that the tank terminal organisation reaps the benefits of the CSMS as soon as possible.'

ONGOING PROCESS

'Tank terminal organisations need to consider that the implementation of a CSMS is not a one-off exercise. Once a CSMS is established, it needs to be maintained in order to be effective.

'There is no need to establish a CSMS if it is not supported or used by the organisation. And a CSMS loses its effectiveness over time, if it does not grow or change with the organisation and does not adjust to changes in legislation, threats and new insights. To ensure that this is the case, metrics (including KPIs) need to be defined and the CSMS needs to be reviewed on a regular basis or when internal or external factors warrant such a review.'

The implementation of a CSMS helps tank terminal organisations to manage, integrate and maintain cyber security and as such comply with current and future regulations and the organisation's vision.

FOR MORE INFORMATION

For more information visit www.hudsoncybertec.com/en/csms