PREPAREDNESS AGAINST CYBER ATTACKS

ONE thing is certain, cyber incidents are a daily occurrence and the response from the public is to generally scorn the organisations involved. For most it seems incomprehensible that such an organisation apparently did not learn from previous incidents or seems to not take cyber security seriously.

THREATS

Cyber security threats for tank terminals are present in all forms. Threats can originate from inside and outside the organisation and are continuously evolving, therefore any tank terminal operational technology (OT) domain cyber security should adjust to the changing threats. Operational personnel must be aware of the latest threats and know what to do in case of an attack. Preparation is key in order to minimise the business and operational impact of a security related incident. Therefore, cyber security should be well integrated in the operation of any tank terminal. Only then, when cyber security has been addressed within the organisation, can you ensure that cyber risks, including disruption in operations (loading/unloading), financial gain (stock manipulation) or industrial espionage (access to confidential data) as well as storage spoofing, ransomware, data leaks and CEO fraud, are managed appropriately.

Besides these targeted attacks, organisations often are 'collateral damage' of an attack and not the intended target of the attack. This is especially the case in industrial chains where one organisation is dependent on another.

STORAGE SPOOFING

One of the threats almost specific to tank terminals is storage spoofing. Storage spoofing is the sale of storage capacity or stock of resources and materials at a tank terminal that do not exist. Storage spoofing attacks are mainly aimed at national and multinational companies that either operate or are looking to acquire storage facilities, but it also targets potential buyers of goods stored at these facilities by masking themselves as legitimate sellers. These goods are offered under false pretences but turn out to be non-existent. Often fake websites that look almost identical to real tank terminal websites are set up to lure potential 'targets' in.

RANSOMWARE

Ransomware is in the news daily and poses a major threat to tank terminals operations. It is a type of malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. This can severely impact a tank terminal's operations and as shown in similar attacks on other sectors, can lead to a situation where the organisation cannot recover from such an attack.

HACKS

Although less common, hacks pose a threat to tank terminals since hacks can have direct an impact on operations. Often hacks are used to take control of or manipulate operations or to steal data and sensitive information. Hacks are more often used to infect organisation's infrastructure with malware, causing a disruption (in the best case) of the primary process.

CEO FRAUD

The threat of CEO fraud is increasing and as such need to be considered by tank terminals since the financial consequences are significant. This is a form of Business Email Compromise attacks (BEC) which use email fraud to attack commercial and other organisations with the goal of obtaining money fraudulently. This type of attack typically targets specific employee roles within an organisation by sending spoof emails that fraudulently represent a senior colleague (CEO or similar) or a trusted customer. Such emails contain instructions to approve payments or release sensitive information. They use social engineering to trick the victim into making money transfers to the bank accounts of the attacker.

HEALTH, SAFETY & ENVIRONMENT (HSE)

HSE risks are an important factor when constructing and operating tank terminals. Tank terminals are built so that HSE risks are minimised. Recent incidents show that even safety systems, used to bring the tank terminal into a safe state in case of an incident, are vulnerable to attack. Once the safety systems are compromised the tank terminal will not be able to return to a safe state in case of an incident. This means that in case the infrastructure is compromised by a hack, a hacker can cause irreparable damage to a tank terminal. In order not to be detected the hacker will, after a successful breach, manipulate existing infrastructure so that the breach is not detected. Based on the point of entry, the malicious hacker has direct access to the OT domain or uses various systems in the IT domain to reach the OT domain.

TAKING CONTROL OF CYBER SECURITY

Tank terminals should be prepared, both on organisational and technical level, for the latest threats and perform cyber security checks regularly. To manage cyber security within a tank terminal organisation, 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 27000 series while the OT-environment can use the international Industrial Automation & Control Systems (IACS) cyber security standard IEC 62443 as a basis to incorporate cyber security within the organisation.

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 that address the three areas of cyber security: people, process and technology.

Tank terminal organisations 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 organisations 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 organisation knows where it stands regarding 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, if any, 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 an organisation's cyber security, a baseline assessment should be performed. The baseline assessment provides the tank terminal organisation with a clear view of the cyber security situation. 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 allows the organisation 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 organisation to identify so called 'quick wins' that can be easily implemented without too much effort.

ONGOING PROCESS

Tank terminal organisations shall be aware that the implementation of a CSMS is not a one-off exercise. Once a CSMS has been established, it needs to be maintained in order to stay effective. There is no need to establish a CSMS if the management system is not used or supported by the organisation. If a CSMS is not used it does not add to the overall security of the tank terminal organisation. If a CSMS does not grow or change with the organisation and does not adjust to changes in legislation, threats and new insights, the CSMS will lose its effectiveness over time. To ensure that the CSMS stays relevant and changes with the tank terminal organisation, 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 within their organisation and as such comply with current and future regulations and the organisation's vision. To ensure that a tank terminal organisation has a flying start and avoids costly mistakes when implementing a CSMS an external expert can support the organisation.

For more information

This article was written by Ilya Tillekens, senior security consultant at Hudson Cybertec.
www.hudsoncybertec.com/en/tsm/