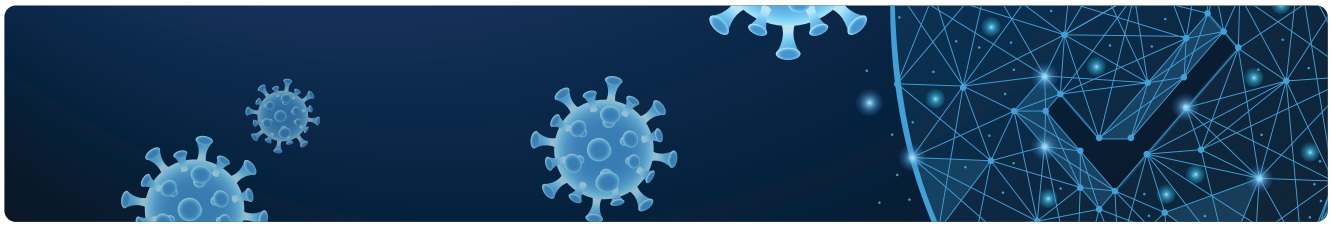
COVID-19: CYBER SECURITY LESSONS LEARNT



THE COVID-19 pandemic has shown us that we need to be prepared to handle extraordinary situations that impact our business when measures to combat the spread of the COVID-19 were put in place by governments worldwide. These measures have had, and continue to have, a major impact in the way that we conduct business and operate our facilities. Organisations often had to fall back on business continuity plans in order to cope with the situation. On top of this, there is an increased threat from cyber-attacks that exploit this extraordinary situation.

PEOPLE

For most tank terminal organisations, there will be minimum staff working onsite. Where possible, staff will work remotely using various means of communication. As the dependence for remote workers on digital infrastructure (supporting video conferencing, online meetings, sharing documents etc.) is increasing, it has an impact on how the tank terminal operates. Working in this situation brings its own risks and opportunities.

It can be observed that as organisations scramble to organize themselves in an attempt to adapt to this situation that, from a cyber security point of view, cyber security not often is considered until 'emergency' infrastructure is in place. Also, existing services have had to adjust to the increasing demand from their customers for online meetings and secure infrastructure such as VPNs (Virtual Private Networks).

Most organisations already had remote infrastructure in place. However, extraordinary demand has uncovered weaknesses in the way that organisations implemented remote infrastructure. These weaknesses are being exploited by malicious actors; therefore, employees should understand the (cyber) risks involved when working remotely.

VPNS AND ONLINE MEETINGS

The usage of VPNs has increased. Organisations that support the usage of a VPN for their remote connections, had to make changes in their infrastructure to meet increased demand overnight.

Increased usage of online meetings showed that certain solutions had major privacy and security issues. Including the ability of non-invited people attending supposedly secure meetings and the usage of personal information by third party social networks.

PROCEDURES

Because of all the changes, for most tank terminal organisations it became evident that normal procedures do not always work or that security procedures are not fully applied when working remotely. For example, solutions were implemented without full compliance with the organisation's security requirements, just to ensure that employees can continue working. Later, when these issues became apparent, additional security measures had to be taken to ensure a secure working environment.

TRAINING

Situations, such as these, show that appropriate (cyber security) training of all people working in your tank terminal organisation is essential. This ensures that everyone knows the cyber related risks and measures when working remotely. For example, only to work from home or another location using your organisation's equipment, to take extra care using remote infrastructure and when using cloud services to be aware that these services can have limitations.

PROCESS

Organisations are rushing to enable large-scale work at home arrangements and educate users about the new risks of remote work. Each tank terminal organisation needs to have their processes, policies, and procedures in place to deal with situations like the COVID-19 pandemic. These must include cyber security since malicious third parties will try to take advantage of such situations. However, quick fixes may cause more problems than the problem it is supposed to resolve. And, at the end requiring more time and resources to resolve compared to a proper solution selection process.

Unfortunately, this is coming at a time when budgets are tightening due to revenue implications presented by the pandemic. The issue here is that expanding your remote workforce while simultaneously cutting budgets regarding cyber security means, for most tank terminals, solving one problem and creating another at the same time. Cutting corners can lead to a critical cyber security breach that would topple the tank terminal operations.

BUSINESS CONTINUITY

This situation clearly shows how important business continuity planning is for a tank terminal organisation. Business continuity planning ensures that the business can continue and survive a disaster such as the COVID-19 pandemic. Every organisation should have a well thought out business continuity plan that encompasses all vital aspects of the business. For cyber security, the recommendations from the IEC 61443 2-1 standard provide guidelines on cyber security that must be incorporated in a business continuity plan.

HANDLING PERSONNEL WORKING REMOTELY

If your organisation relies on third party infrastructure like cloud services and secure (VPN) connections, you should ensure that these services comply with your organisation's minimum

requirements for business operations. If the need arises to scale up in remote access or other areas, you need to ensure that you have both the infrastructure and resources available in order to do so in a timely manner.

In addition, tank terminal organisations should consider how to protect their equipment (like a laptop or tablet) to be used remotely from the employees' home environment and infrastructure. Also, they should consider how policies and procedures will be enforced.

This means that the appropriate processes, policies and procedures need to be in place and must have been tested to ensure that your organisation can continue operations. Things to consider are among others: how can we communicate (securely), what are the limitations of our infrastructure and what is the impact etc.

TECHNOLOGY

As a result of this pandemic, trusted technologies may no longer hold up under new pressures and might need change to accommodate the new requirements.

INCREASED ATTACK SURFACE

Having many of your employees working remotely increases the attack surface of your organisation. How do you manage the security of your remote employees? Defending against new phishing and malware campaigns might become a priority, as criminals will take advantage of the panic.

'Recommendations from IEC 61443 2-1 provide guidelines on cyber security that must be incorporated in a business continuity plan'

Ideally all remote users will have a VPN, but during this pandemic, this is not always the case. For example, users using popular (free) video communication tools. Therefore, it is important to monitor your now extended infrastructure for any security flaws and breaches. Is your current monitoring and logging solution up to the task?

PROTECTING INFRASTRUCTURE

A (remote) security operations centre can ensure that your critical infrastructure is being monitored and secured when a tank terminal organisation has minimum staff onsite. Since well managed cyber security is a vital part of your tank terminal organisation's defences, continuous monitoring for potential breaches is a must for protecting the assets and intellectual property.

Be aware the (remote) security operations centre is specifically setup and capable of monitoring your tank terminal's operational technology (OT) to ensure your business critical OT environment is protected against cyber related incidents.

Tank terminal organisations should incorporate the 'lessons learned' from this pandemic and incorporate them in the existing cyber security management system. Or, setup such a system in case this has not been done yet. At least the impact of the lessons learned should be reflected in an updated business continuity plan and existing measures should be evaluated and updated if needed.

For more information

This article was written by Ilya Tillekens, senior security consultant at Hudson Cybertec. Hudson Cybertec is the independent cyber security consultancy & services provider for operational technology (IACS) specialized in critical infrastructure, including the tank terminal sector. For more information please visit www.hudsoncybertec.com/en/tsm