Invisible threat

Increasingly sophisticated attacks mean no business can underestimate the importance of cybersecurity. Complex industrial control systems are no exception.

What are your company's most important assets? Data, whether it concerns employees, operations or suppliers, is undoubtedly among the most crucial. Which makes protecting that data an integral part of any business. By accessing valuable data, cyber criminals can threaten operations and steal valuable information. And in the age of big data, cloud storage, mobile devices and the Internet of Things, the sheer number of access points to safeguard can be overwhelming.

The complexity of the machinery and processes involved can make industrial plants a vulnerable target, particularly as they progress along the path of digital transformation, connecting information technology (IT) with operational technology (OT). Evaluating the risks for the many devices and then securing these systems can be a complex process. And as processes become increasingly interlinked, businesses also need to be aware of the precautions taken by suppliers and customers. You are only as strong as your weakest link.

DISASTROUS CONSEQUENCES

The effects of a data breach can be disastrous. In 2014, hackers gained access to the industrial control system of a steel mill in Germany. They prevented the shutdown of a blast furnace, resulting in major damage to the plant. And it is not just isolated incidents that pose a threat: In 2017, the WannaCry virus disrupted information systems at hospitals, banks, railways and car manufacturers in more than 100 countries.

Cybercrime can take many different forms, leading to manipulation or loss of data that can affect production and damage a company's performance and reputation. Cybersecurity seeks to protect the confidentiality, integrity and availability of data.

ANDRITZ UNDERSTANDS CYBERSECURITY

ANDRITZ knows about the importance of secure industrial operations and is constantly looking to enhance its growing cybersecurity solutions. "It means a lot to us to ensure reliable and safe growth of digital productivity," says Klaus Glatz, ANDRITZ Chief Digital Officer.

In December 2017, the company began a partnership with OTORIO, a leading cybersecurity provider for digital transformation. "As well as using their expertise to protect our own operations, we are also offering it to our customers and new customer groups," says Glatz.

CUSTOMIZED SOLUTIONS TO SUPPORT DIGITIZATION

Generic solutions have limited ability to prevent cyberattacks affecting the production floor. This is due to the inherent uniqueness of the OT environment. ANDRITZ is embedding OTORIO's innovative solutions in its market-leading products and services, ensuring every machine meets the highest standard of cybersecurity. Safe digitalization requires a holistic end-to-end approach, from the development phase to ongoing operations, which is why ANDRITZ and OTORIO have developed an extensive cybersecurity program ranging from advanced assessments and consulting services to the implementation of proven cybersecurity and risk management technologies.

"In a constantly changing threat environment, customized operational technology cybersecurity measures are an essential part of the automation development process,"

adds Klaus Glatz.

The advanced services ensure continuous, efficient and effective production alongside proprietary commercial data security. Ongoing risk monitoring and management is enabled by security orchestration, automation, and response (SOAR) machine power. Valuable additional tools are also provided, including a platform to coordinate all IT/OT security tasks, an offline platform that uncovers cyber risks resulting from the supply chain, and an encrypted and secure communication channel for accessing the OT network. •

OTORIO – WHAT YOU NEED TO KNOW

- Founded in December 2017 as a partnership between the OTORIO management and ANDRITZ AG (majority share)
- Location: Tel Aviv, Israel
- Employees: 50+
- Business: Cybersecurity solutions for industrial manufacturing companies

"The main challenge for the industries is to understand that cybersecurity is not a purely technical issue. Although it has technical aspects, it should be identified, monitored, quantified, and continuously managed."

Daniel Bren, CEO OTORIO

FACTS ABOUT CYBERCRIME

$1.5 trillion
Cyberattacks cost businesses at least US$1.5 trillion per year

67% increase
Attacks have increased by 67% in the past five years

43%
...of these attacks are targeted at middle-sized companies

14 seconds
On average, there is a ransomware attack every 14 seconds