VerticalStructure

ADVANCED MANUFACTURING CASE STUDY

Cyber Security and Industry 4.0

CYBER SECURITY & INDUSTRY 4.0 - BACKGROUND

In 2017, Mondelez, the multinational food and beverage company, suffered an attack that leveraged the encrypting malware NotPetya

Key points:
The attack

- **permanently damaged 1,700 servers and 24,000 laptops**
- **impacted production facilities around the globe**
- **included the theft of thousands of user credentials**
- **impacted the company's ability to complete customer orders.**

It cost Mondelez $100 million.

The NotPetya attack also damaged operations at Maersk, which lost $300 million, at FedEx, which lost $400 million, and at Rosneft, a Russian oil company.

The White House estimated that NotPetya generated $10 billion in damages. (*https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/)*
.

We know that every connected device represents a potential risk. A security-first approach is critical as organisations move from legacy systems and traditional processes, to take advantage of "smart" and advanced technologies, such as the Internet of Things.

Simon Whittaker
Co founder & CEO
Vertical Structure

OVERVIEW

Our client is a complete automation technology supplier operating internationally. It is a provider of products, systems and services in all aspects of automation, driving the smart factories of the fourth industrial revolution. Vertical Structure (VSL) has been working with the team at its Ireland campus since 2020.

THE CHALLENGE

Like many manufacturers, it is embracing digitisation, the Internet of Things (IoT) and Industry 4.0. However the sector is considered a high-value target by cybercriminals. The challenge faced by the team was to secure smart manufacturing systems.

They recognised that security had to play a key role underpinning the development of future smart manufacturing systems.

WHY THEY CHOOSE VERTICAL STRUCTURE

Vertical Structure (VSL) has worked with companies embracing Industry 4.0, so the team knows the challenges the sector faces and how to address them.

For instance, the team is experienced in securing **operational technology**, such as, Industrial Control Systems (ICS), Supervisory Control & Data Acquisition (SCADA) and Distributed Control Systems (DCS), as well as IT systems.

Our client was looking for a knowledgeable partner, but also one who could communicate easily with people from all divisions of the business. The Vertical Structure team has a pragmatic and personable approach to cyber security.

THE SOLUTION

We completed penetration testing, carried out threat modelling exercises, produced security documentation that everyone could understand, offered input at an executive level on cyber, and helped improve knowledge of cyber within the company.

1

EVALUATED SECURITY

Every piece of software, whether developed internally or from a third party is regarded by the client as external, in terms of ensuring it is secure. The VSL team carried out controlled penetration testing to evaluate the security of the client's own internal SaaS platform based in AWS, IoT systems and other cloud based infrastructure. The focus was then on leveraging the deep experience of VSL's security and penetration testers to highlight areas for improvement.

2

IDENTIFIED, ENUMERATED, MITIGATED THREATS

VSL worked with the client on a comprehensive threat modelling exercise. This identified potential threats, such as structural vulnerabilities and the absence of appropriate safeguards. This made it possible to clearly see what the impact of these threats could be, and, with that in mind, mitigations prioritised and plans produced on how to deal with incidents if they did occur.

3

CREATED CLEAR INFORMATION

VSL produced security analysis documentation for the client. This was clear information and security best practices about complex products, machinery, software and processes. The security documentation delivers significant value - reducing risks, and supporting digital transformation, so it was written to be usable and accessible, accurate and up to date.

4

ADVISED ON THE IMPACT OF SECURITY ON STRATEGY

As our client embraces the Internet of Things and Industry 4.0 VSL was able to give guidance to make sure cyber security was given proper consideration. The team carried out an initial review of the AWS® security and infrastructure requirements; security testing of all areas of the client's web application including implementation of cloud systems; and a final security testing of AWS® environment.

5

IMPROVED COMPANY CULTURE & KNOWLEDGE OF SECURITY

"Cyber security" isn't a one off tick box exercise. Our client realised the importance of having a skilled up team and engaged VSL to run interactive training sessions on Threat Modelling & Web Application Security, so it was in a position to protect itself from vulnerabilities and common attacks. VSL also ran Cloud Application Security Testing training. This gave the client a practical understanding of securing software deployed into cloud environments and gave them an understanding of the issues and opportunities presented by serverless solutions.

We are committed to remaining at the forefront of innovation. We know that adopting Industry 4.0 technologies goes absolutely hand in hand with a robust cyber security strategy. Vertical Structure helped us at a tactical and executive level to deliver that strategy.

Client's Software Test & QA Manager