Case Study

CYBERSECURITY FOR INDUSTRY 4.0

Keywords: *Cyber-security, technology, cyber-attacks, safety*

Background to Case Study

The large amount of new technology, creates opportunities and spaces for cyber-attacks, that why ensuring cybersecurity is crucial for Industry 4.0 to succeed. It is really important for organisations to update its knowledge and tools to meet the future challenges.

Most industrial environments were not designed with high cybersecurity in mind. Manufacturing systems are now moving towards cyber-physical systems, where any vulnerabilities could be detected and exploited by malicious individuals.

Introduction to the Case Study and it’s growth within Industry 4.0.

Cyber-security is still associated with protection against viruses or malware, but nowadays the scale and threat are definitely more global. There are more and more financial crimes or acts of espionage, but there are even attacks on critical infrastructure, governments. To minimize the threat and take advantage of the opportunities offered by Industry 4.0, it is necessary to disseminate and apply good practices to protect against cyber threats.

Digital security must be the result of a comprehensive IT content management policy and the enhancement of user competence. The human factor is more challenging than the infrastructure factor, because the most common reason for getting data out of the workplace is the use of users, e.g. by using private mail or connecting unauthorized data carriers. Companies incur real financial losses in case of commercial and industrial information leakage.

Data protection therefore starts with the implementation and enforcement of security rules from employees.

Project No. 2019-1-PL01-KA202-064936

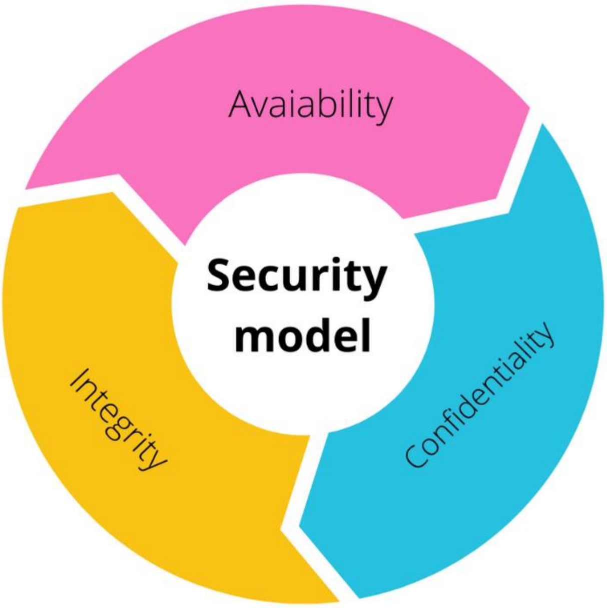
The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the Erasmus+ Programme of the European Union

The Case Study and Industry 4.0 Elements: A Pictorial Overview

Global Networking and Industry 4.0 opens up new opportunities for communication and information exchange, but inadequate security can carry a number of serious risks and financial losses. Safety is a process in which a set of activities is constantly performed. One of the models describing safety is the CIA model which each company should define, observe and maintain.

The CIA security model is based on three basic elements:
- Confidentiality - data and services should be accessible only to those who have the right to them
- Integrity - any attempt to compromise data and services should be detected and recorded
- Availability - whoever is entitled should be able to use the resources.



Project No. 2019-1-PL01-KA202-064936

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the Erasmus+ Programme of the European Union

Case Study

CYBERSECURITY FOR INDUSTRY 4.0

The Element Explored within Industry 4.0 Application.

Polski Tytoń Dystrybucja is one of the largest FMCG and tobacco products distributors in Poland. It offers logistic and trade services. The sale is carried out in the Sales Department and through sales representatives, who reach the customers directly. The company is constantly working to improve the quality of its services in order to best suit the demanding customer. In order to provide services at the highest level it invests in staff training and modernization of the system.

Polski Tytoń has implemented the Axence nVision management system, which enables the administration and ongoing reporting on the status of each of the devices connected to the network, thus increasing the security level of the company's IT infrastructure.

The main challenge in the company was to find a tool that would allow to control the processes taking place in the network in individual branches. Another area that needed to be improved was the monitoring of hardware resources in the server room and individual workstations as well as the use of computers and network devices by employees.

Since the implementation of this solution, the company has been able to work with a remote console, which allows defined administrators to access the program from any computer, this facilitates ongoing monitoring of application parameters, viewing the event log or system services. The use of Network modules limits the connection of external private devices and also allows to monitor environmental conditions in the server room, which provides protection against failures.

The administrator is informed in case of a dangerous increase in server temperature or lack of disk space. The company has also limited the display of social profiles and Youtube service, which has had a positive impact on employee performance.

The implementation of this solution has brought the company many results:
- Improvement of transparency and corporate usability,
- The IT department has been given access to monitor all processes taking place in the network,
- Insight into the data collected and analysed by the system,
- Easy detection of malfunctions of all devices,

Project No. 2019-1-PL01-KA202-064936

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the Erasmus+ Programme of the European Union

	- Reduction of IT infrastructure maintenance and maintenance costs, *- Increasing the efficiency of technical assistance,* *- Control over the operation and use of the network,* *- Increased efficiency of business processes,* *- Saves time by being able to react quickly to system errors and provide remote assistance to employees.*
Application Target Audience	*The results of the case-study are intended for use by SMEs, Enterprises and Entrepreneurs.*
Resources Used:	*https://axence.net/files/pdf/media/case_study_polski_tyton.pdf* *http://ptdystrybucja.pl/o-firmie/*
Further Reading:	*https://ik.org.pl/wp-content/uploads/wyzwania-w-cyberprzestrzeni.-przyklady-rozwiazan-zagrozenia-regulacje.pdf* *https://axence.net/pl/o-nas* *http://websecurity.pl/pojecie-bezpieczenstwa-cia/*

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the Erasmus+ Programme of the European Union