Increasing the Competence and Resilience of Industrial Cybernetics by Involving the University Environment

Florin POPESCU
Carol I National Defense University, Bucharest
popescu.vflorin@unap.ro
Olivia COMȘA
SAFETCH Innovations, Bucharest
olivia.comsa@safetech.ro

Abstract: The evolution of modern society is inconceivable today without digital development. From easier access to internet to the services and industries digitization and the development of sophisticated critical infrastructure, all involve the extensive use of digital services and internet. In addition to the benefits of fast access to documents and information, the danger of cyber-attacks is gradually increasing. As there are no physical borders for the digital world, since 2021 Romania is a new participant in the creation of the "European Industrial, Technological and Research Center on Cyber Security" and a regional player of international importance in this process. Thus, cyber security is no longer just a technological option, but also a societal need. Cyber threats are no longer limited to cybercrime, but have become a subject of national security. To meet these challenges in the context of the accelerated services and industries digitization has become crucial for the creation of a cyber security ecosystem through a public-private partnership between authorities, research centers, universities and the private sector in order to increase the resilience of critical infrastructure and to promote research, innovation and technology transfer.
Keywords: Industrial cybernetics, SCADA, OT, IT, University Cyber Range, Virtual platforms.

INTRODUCTION

Day by day, there is a multitude of announcements coming from various government agencies, private companies or ordinary users regarding the damage caused by various cyber-attacks, which not only cause material and / or image damages, but also significant vulnerabilities and security breaches. The current need for specialized staff is crucial at all levels, from private companies to essential service operators and government systems. Estimates of responsible bodies and specialized companies indicate a deficit of several million jobs in cyber security, a deficit in permanent growth. The solutions of providing specialized human resources are different from country to country, from institution to institution. By and large, most of the approaches take into account the involvement of the expertise coming from all exponents of education and training within the university, public and private environment, in order to increase professional competence. In this respect, the training of

students, masters, specialists, as well as the establishment of new occupational standards in the field of cyber security in the industrial environment have become imperative and must be completed with the help of the university programs.

ANALYSIS OF ENSURING INDUSTRIAL CYBER SECURITY IN EUROPE

According to a statement from the computer security company Kaspersky, industrial organizations are currently facing a challenge - the protection of industrial control systems (ICS) that must face a wide range of attacks (Kasperski, 2019).

In 2020, in the study Cooperation between CSIRTs and Industrial Control Systems (ICSs) community, ENISA worked on a report on good practice and recommendations needed to harmonize a European-wide certification scheme for ICS (Industrial Control Systems) / SCADA (Supervisory Control and Data Acquisition) necessary to certify security experts.

The conclusions of this study highlight that in Europe, ICS / SCADA systems are not at the level of development and use as they are in the North American continent. Because of this, the regulations are a bit behind. Netherlands, Germany, Sweden and UK are the countries that have made some progress in this case. A summary of the main regulations is shown within Table 1.

However, ICS / SCADA security is not limited to the protection of data red by a meter („accounting controls"). For example, computers which manage the flow of electricity at the level of a region are also considered.

In the report "Communication network dependencies for ICS/SCADA Systems" (ENISA, 2017), the most common vulnerabilities of industrial control systems are presented, from which the most relevant have been selected:

- Lack of network monitoring mechanisms - the use of Intrusion Detection Systems (IDS), along with antivirus and firewall solutions increase the security of the infrastructure, as long as the protocols specific to SCADA systems are understood in the analysis process;
- Misunderstanding the content of vehicular traffic - identifying sophisticated cyber threats such as APT (Advanced Persistent Threat) requires, first of all, knowledge of the network traffic in order to separate abnormal behavior from legitimate traffic;
- Poorly trained IT administrators in cyber security - usually, the staff engaged with tasks in the management of a SCADA infrastructure considers the identification of incidents that could affect the cyber security of the infrastructure to be optional;
- Use of operating systems that are vulnerable or no longer supported - in an infrastructure that manages industrial control systems, an important role is played by the

NIST SGIP-CSWG		Smart Grid Interoperability Panel – Cyber Security Working Group
NERC CIP		Cyber Security Regulation for North American Power Utilities
IEC 62351		Data and Communications Security
IEEE PSRC H13		Cyber Security Requirements for Substation Automation, Protection and Control Systems
IEEE 1686		IEEE Standard for Substation Intelligent Electronic Devices (IEDs)
ISA S99		Industrial Automation and Control System Security
ICSJWG		Industrial Control System Joint Working Group

Table 1: *The EU main regulations in the field of industrial cyber security*

uniform application of updates which remedy cyber vulnerabilities identified by the manufacturer. Often, there occurs situation where, for reasons related to the age of the hardware components, the operating system does not support updates. In this case, changing the equipment involves costs.

- Uneven application of security updates at the level of computer equipment - the application of updates must be done in a uniform way to ensure an optimal level of cyber security. This activity requires a good management of the equipment by IT administrator, the data about the number of managed equipment as well as their characteristics (hardware and software) being necessary;
- Installation of irrelevant software applications on systems of major importance in the SCADA network - in this situation, systems with a key role in a SCADA network should not be loaded with unused applications because, in some cases, they can generate cyber vulnerabilities by not updating them regularly;
- Poor implementation of remote communication channels - remote communications are a possible gateway for an attacker to enter an infrastructure. Therefore, equipment that is used for such activities must have a higher level of security and restricted physical access;
- Data transmission via wireless connections - implementing such connections can facilitate the interception of data by an attacker, generating multiple risks if the data is encrypted insufficiently or incorrectly;
- Exposing in the public space of elements or data related to the architecture of the SCADA network - exposure of such data can lead to their use in the reconnaissance stage in the course of a cyber-attack, according to Cyber Kill Chain (Lockheedmartin, 2020);
- Infrastructure developed around the concept of "security by obscurity" or based on trust, in isolation from the internet network - decisions that often turn out to be wrong. The infrastructure can be penetrated by an attacker and by „offline" methods.

Regarding the situation in Romania, companies headquartered in our country have planned spending on cybersecurity solutions up to 14% compared to 2020 when the percentage was 11%, according to a study by SAFETECH Innovation (Bussiness Magazine, 2011).

DISCUSSIONS AND PROPOSALS REGARDING THE INSURANCE OF INDUSTRIAL CYBER SECURITY

Regarding the Operational Technology (OT) cyber security matrix, in United States of America there are more than 30 standards, guidelines and frameworks for industrial cyber security and critical infrastructure. Understanding the differences between them is not a minor task. In order to protect industrial networks effectively and efficiently, a methodological and scientific approach has become crucial.

Who is responsible for industrial cyber security?

In Europe and, implicitly, in Romania, the responsibility regarding the industrial cyber security is not very clearly delimited conceptually and practically. But what is very clear is the need to prepare and certify an entire chain of actors that must add value to the concept of industrial cyber security, as follows:

- End users: the first step is to define policies, procedures, specifications, etc. as part of a good and efficient cyber security industrial program;
- System integrators: system integrators need to understand vendor specifications and requirements related to industrial cyber security;
- Industrial system vendors: system vendors must provide and maintain vulnerability-free systems that meet current security needs;
- University and research environment: Educational institutions will need to improve the way they conduct their cyber security research through the use of SCADA systems, similar to those used in industry.

Proposals regarding the involvement of the university environment for ensuring industrial cyber security:

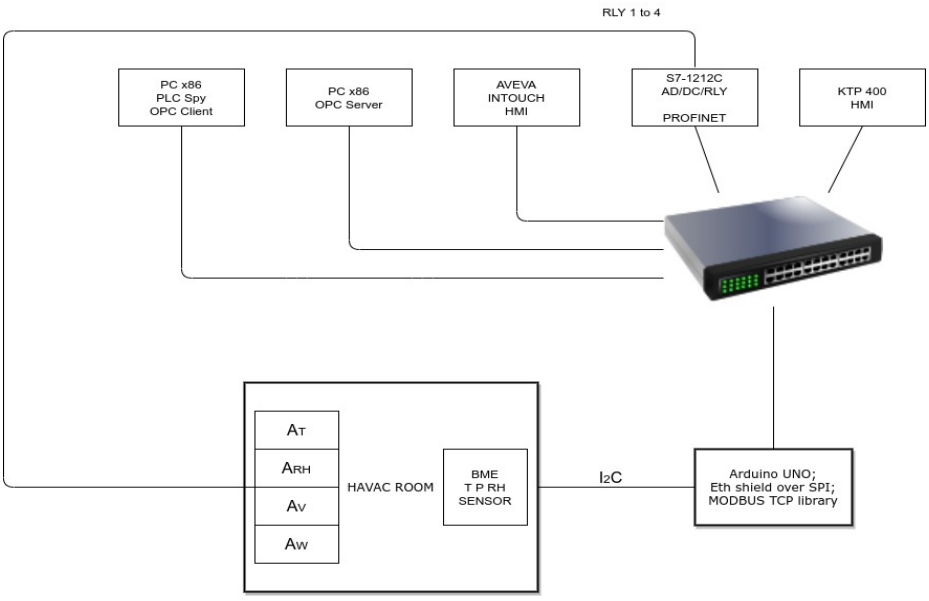
- Creating an up-to-date course base for current needs and preparing human capital in collaboration with the „European Cybersecurity Industrial, Technological and Research Competence Center" for the transmission of theoretical and practical knowledge in the field of information security for future generations of students and master students, as well as the ability to develop an information security system for their own organization and a permanent CTF competition: International Students Contest on Information Security (Suceava University, 2020);
- Integration of cyber polygons in universities, such as the ones operating at University POLITEHNICA of Bucharest and at the National Defense University in a common platform for analyzing industrial cyber security;
- Integration of innovative solutions such as automatic implementation of virtual machine parameters with laboratory activity, based on customized templates adapted to the user profile / curriculum / topic / activity, at the moment of implementation;
- Creating new generations of blended learning training scenarios which facilitate easier learning by simulating real-life scenarios, mainly ICS-SCADA security.

Proposals regarding the standardization of a typology of research laboratories for Industrial cyber security in universities:

Cyber Laboratories, like the one from Carol I National Defense University developed through SAFEPIC 19 project, should include an enclosure with sensors that monitor values such as temperature, pressure, humidity, but also on / off actuators (heater, fan, solenoid valve) which will be controlled by certain thresholds values transmitted by sensors, but also according to a predefined function and with day-night cyclicity.

The proposed architecture provides the necessary flexibility to organize complex exercises and experiments in the field of cyber security. The solution also allows a partner to specialize in a specific field (for example: SCADA, mobile devices, IoT) and the other partners to access the resources developed by that partner. In addition, the scenarios and exercises developed by one partner will be ported and used by the other partners to train their own students. A model of a process diagram is presented in Figure 1.

Fig.1: *A model of implementing cyber range at Carol I National Defense University*



The equipment and software that should be installed / configured within the services are the following:

- OPC server - process control and supervision server;
- InTouch HMI - global operating interface;
- Siemens S7 1212C PLC - process controller;
- HMI Siemens KTP 400 - local operator interface.

The stages of conceptualization, simulation, testing and validation of the equipment in the cyber range will be performed in stages by the end of 2021. The result of implementing the cybernetic polygon from Carol I National Defense University will be a platform used to test the security of simulated networks. The platform can test the resilience of systems to cyber-attacks in environments similar to the real ones and evaluate the capabilities of offensive or defensive solutions.

CONCLUSIONS

Unfortunately, the speed of technology evolution is not followed by developments in the education and training system in order to ensure sufficient human resources, specialists and capabilities needed to enable secure cyber governance. The result of the deployment of cyber polygons as a platform similar to the European initiative FIRE (Future Internet Research and Experimentation) to achieve a standardized research and testing environment in cyber security will lead to the creation of a virtual environment which allows „players" to carry out cyber-attacks. By interacting with these polygons, students can learn offensive and defensive techniques and tactics to identify and exploit vulnerabilities in virtual infrastructure, as well as methods to secure systems and conduct digital investigations. The scenarios will be developed on various levels of difficulty and will allow the accumulation of knowledge and increase the level of expertise of the participants. The cyber platform will also be used by government agencies, contractors or companies that manage critical infrastructure (energy, water, gas, fuel, etc.) and thus they could assess the security of their systems at low cost.

AKNOWLEDGEMENTS

This paper was published in the project „Center of Excellence for Cyber Security and Critical Infrastructure Resilience (SafePIC)" contract no. 270 / 23.06.2020, ID 120436, financed under the Operational Program Competitiveness 2014-2020, Priority Axis: 1. Research, technological development and innovation (RDI) in support of economic competitiveness and business development.

REFERENCE LIST

Business magazine (2021). Companiile româneşti majorează cheltuielile pentru soluţiile de securitate cibernetică la aproape 14% din bugetul IT, faţă de 11% în 2020. Accessed on 17th February 2021 at https://www.businessmagazin.ro/actualitate/companiile-romanesti-majoreaza-cheltuielile-pentru-solutiile-de-19853516

ENISA (2017). Communication network dependencies for ICS/SCADA Systems. Accessed on 23rd March 2021 at https://www.enisa.europa.eu/publications/ics-scada-dependencies

ENISA (2020). Cooperation between CSIRTs and Industrial Control Systems (ICSs) community. Accessed at 24th of March 2021. https://www.enisa.europa.eu/topics/cross-cooperation-for-csirts/scada

Kaspersky (2019). Industrial Cybersecurity in Practice. Accessed on 21st March 2021 at https://ics.kaspersky.com/trainings-and-awareness/#collaboration

Lockheedmartin (2020). Cyber Kill Chain. Accessed on 22nd March 2021 at https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Suceava University (2020). International Students Contest on Information Security. Accessed on 20th March 2021 at https://ctf.usv.ro/