BUILDING A CONCEPT FOR CYBER SECURITY OF AN EDUCATIONAL ORGANIZATION IN BULGARIA

Katya Emilova Kirilova[1]

Abstract: Background: The topic of cyber security of organizations is becoming more relevant for modern societies. In that area, both scientific research and practical applications of various platforms, technologies, and tools for guaranteeing security levels have undergone serious development in recent years. The research objective is based on a study of leading literature sources and the accumulated experience in the subject area to propose and approve an adequate model for ensuring cyber security of an educational institution. Methods: Different organizations adopt different approaches and apply different methods to create systemic conditions for ensuring cyber security. The methods used in the research are based on the specifics of the business processes that take place in the organizations. Based on them, the specifics of educational organizations are highlighted, which determine the creation of a relevant concept of cyber security with appropriate technological measures. Results: The concept proposed in the present study is based both on the current legal framework of the European Union and the Republic of Bulgaria, as well as on good practices and approaches in the subject area. The concept has been implemented and the presented results prove its usefulness for the educational organization. The period to which the empirical part of the study refers is 2022-2023. Conclusions: The main results of the study are in the direction of achieved monitoring of the external perimeter of the organization, implemented monitoring of user behaviour, risk management of information assets, and increased cyber security of the organization.

Key words: cyber security, cyber threats, cyber security concept, technological protection measures

JEL: K24, L86, P46.

DOI: https://doi.org/10.58861/tae.bm.2024.1.05

[1] Assoc. Prof., PhD, University of National and World Economy – Sofia, e-mail: katia.kirilova@unwe.bg, ORCID: 0000-0002-1975-3657

Introduction

In modern living conditions and dynamically developing social processes, the ability to provide services in a safe digital environment is essential for educational organizations. The main requirement in this direction is for organizations to take measures for a high degree of security and ensuring the protection of sensitive information, which is an asset for organizations. In the research, we support the understanding that the effectiveness of higher education in Bulgaria is extremely important (Kirilov, 2020). The fact that educational organizations are administrators of personal data places them in a situation of implementation of several regulations providing provisions for protection of personal data. Personal data breach means a security breach that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access of personal data that is transmitted, stored, or otherwise processed (GDPR, 2016). The challenges of handling personal data (Majeed, 2023) facing public sector organizations, particularly educational organizations in the digital age, are a priority of paramount importance given the criticality of the infrastructure and the sensitivity of the information. Several organizations in the public sector are subject to cyber-attacks (Stone, 2023) due to the information assets and the large volume of sensitive information at their disposal. The fight against cyber threats also includes specially created organizations that help develop cyber security by bringing together the public and private sectors (ECSO, 2023).

The constantly developing possibilities of the digital space provide conditions for improving the activities of educational organizations, but on the other hand, they create an environment for the growth of malicious actions and the realization of cyber-attacks. By their nature, they are targeted, malicious actions targeting organizations' sensitive information and critical infrastructure. They mainly address computer systems and networks, including smart networks (Bouramdane, 2023) and aim to gain access to and provide control over an organization's sensitive information.

The application of a conceptual approach, through which the educational organization defines its framework of protection in cyberspace and outlines the main directions of action, is important in building network and information security and preserving the confidentiality, integrity, and accessibility of information. Given the specific field of activity of educational organizations and the related processes of processing, storage, distribution and administration of sensitive data, network and information security are a priority for several governments (Alrubaiq, 2021). Faced with the risk of

cyber-attacks, organizations are faced with the need to take measures to reduce and eliminate risks, prevent cyber-attacks and ensure effective network and information security. A step in this direction is the fulfillment of the requirements of international certificates and the definition of control mechanisms, according to which an information security management system is built and implemented (Antunes et al., 2021). The process of certification of educational organizations provides a clear vision and application of a systematized approach to building the cyber security of the organization by introducing an information security management system that provides the control mechanisms to protect the sensitivity of confidential information. (ISO, 2023). The main guidelines for ensuring compliance with the requirements of international standards are understanding the context of the organization's existence, its needs and requirements, as well as the relationships in the surrounding environment. This should only happen with clear leadership and commitment from management. The decision on this step, as well as the undertaking of several measures in this direction, are the subject of activity of the management of the organizations. Management decisions regarding subordination, de-centralization and responsibilities play an essential role in the functioning of educational organizations and the need to build their cyber security. In the context of improving management decisions that are made in organizations, it is essential to have data in a form that allows their subsequent analytical processing (Milev et al., 2022). The relationships between structural units, the performance of activities and the efficient use of resources are inter-connected and threatened by cyber-attacks in their interconnectedness. Everything stated gives us grounds for building a conceptual model of the cyber security system of an educational organization.

Materials and Methods

Applicable European and National Legislation

In recent years, the European Union has been developing a consistent and targeted policy to improve cyber security at all levels in organizations. The main regulatory body is the European Union Agency for Cybersecurity (ENISA, 2023). It was established in 2004 with Regulation (EC) No 460/2004 of the European Parliament. In the Republic of Bulgaria, the NIS directive has been transposed into the national legislation, through the Ordinance on the minimum requirements for network and information security (Ministry of

Transport and Communications of the Republic of Bulgaria, 2023). Now, the increased requirements that are introduced with NIS2 have not yet been transposed into the national legislation of Bulgaria. This process is pending. Therefore, the construction of cyber security concepts in organizations should be based on both the current national legislation and the new European directives, which have not yet been implemented in the practical work of the country.

Cybersecurity system of an educational organization

To be able to create a concept for cyber security of an educational organization, some of the specific features of educational organizations should be considered, namely: large number of users; a wide variety of information assets; large building stock. Considering these characteristics of educational organizations, a complex conceptual model for cyber security of an educational organization can be applied, including the following four-layer architecture (Figure 1).

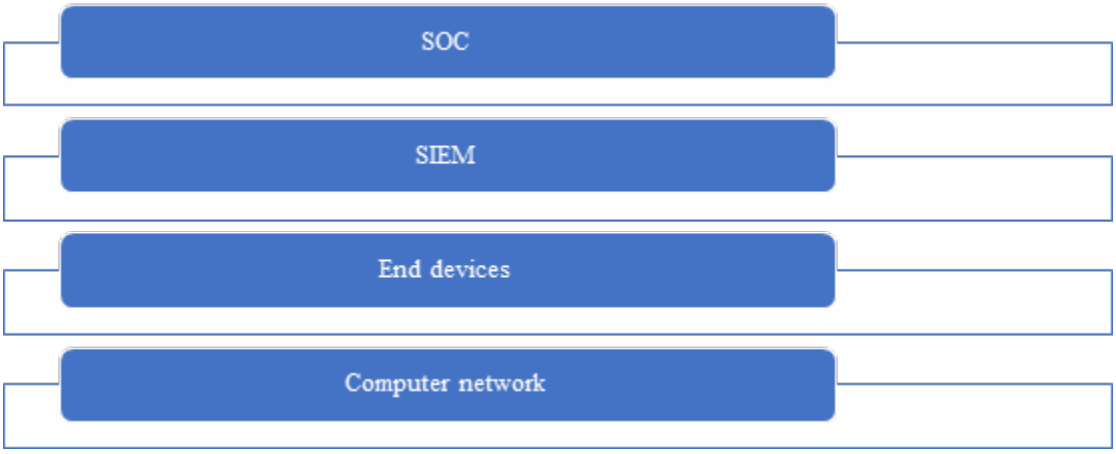


Figure 1. Cybersecurity concept

The first layer is the computer network. At this layer, it is very important to correctly define the network diagram of the organization. Network management implements some of the minimum requirements for network security.

The second layer is the end devices. Endpoint security software must be installed and supported on them. According to Gartner (Gartner, 2023), one of the suitable software for providing Endpoint protection is ESET PROTECT. ESET provides multi-layered protection, including both components of leading antivirus technology, as well as effective protection

for online shopping and payments (ESET, 2023). Comparing this product with other similar alternatives also shows very well provided features of ESET. For example, a comparison with Symantec Endpoint Security and Cisco AnyConnect shows the great functional superiority of ESET (Capterra, 2023). Securing all elements of an organization's cybersecurity with end-point protection software enables the implementation of the third layer of an educational organization's proposed cybersecurity system, namely SIEM.

The third layer of the proposed concept of cyber security of an educational organization includes a Security Information and Event Management (SIEM) system. According to data from Gartner, Security Information and Event Management (SIEM) technology supports threat detection, compliance and security incident management through the collection and analysis (both near-real-time and historical) of security-related events, as well as a wide variety of other event and contextual data sources (Gartner, 2023). The application of this type of centralized monitoring platform is possible only by ensuring a permanent connection of the SIEM with the Endpoint protection software. A very important feature of this type of systems is the ability to process data both in real time and for past periods characterized as historical data. In the specific concept of cyber security, the use of Rapid7 (Rapid7, 2023) is proposed.

The fourth layer of the proposed concept of cyber security of an educational organization includes the Security Operational Center as a service delivery tool. This information service provides 24/7 monitoring of all cybersecurity components and the organization's external perimeter.

Roles and responsibilities of cyber security system participants

In connection with the proposed concept of cyber security, it is important to emphasize the leading role of human resources in the process of its implementation and use. In this way, it is perceived that the separation between the roles and responsibilities of the individual participants in the process is a key prerequisite for achieving the maximum result. As an element of the concept, we offer the following main groups of participants:

The organization's cybersecurity manager. In cybersecurity standards, as well as based on the good practices of leading organizations, this track is key to solving all conceptual and practical issues of implementing the system of organizational, technical, and technological means of protection. The manager’s functions should be implemented in the following directions: Development of the information security policy of the educational organization; Developing and proposing procedures for changes in means of

information processing; Offers and monitors the implementation of measures to prevent and detect the introduction of malicious software; Controls the use of permitted software in the educational organization; Develops procedures for system redundancy and overall storage of regulated periodic backup copies; Monitors and controls the safe operation of software applications in the organization; Monitors the regular keeping and storage of system documentation; Develops the control mechanisms and monitors their application, regarding the rights and privileges of access to the information systems, application and network services owned by the organization; Introduces and controls access to the physical areas with information on the territory of the educational organization; Creates and monitors the application of means and mechanisms when using portable computers and remote work tools; Proposes and periodically analyzes the operation of the information systems based on the risk assessment; Develops and periodically analyzes the use of cryptographic control mechanisms; Monitors the strict implementation of incident reporting procedures, according to established rules; Develops and offers maintenance and recovery activities for all means of information processing, in the event of disasters, accidents and unforeseen situations; Monitors and with particular attention analyzes the organization's critical business processes; Creates mechanisms for periodic review of vulnerabilities of the organization's information systems; Performs methodological guidance on all issues related to cyber security management; Initiates proposals for amendment and improvement in the cyber security system.

Cyber Security System Manager. The manager’s functions are limited to the development and maintenance of system application documentation from the point of view of regulatory requirements. The systematization of responsibilities for this role includes: Ensuring that the concept of cyber security is implemented in the educational organization in full compliance with regulatory requirements; Maintains communication with the management of the organization and reports on; Takes action to perform corrective actions in the operation of the system; Makes operational decisions on issues related to cyber security management; Participates in the determination and adoption of the risk assessment methodology.

Technology and Systems Manager. This role in the system is also important. It is mainly measured by the high degree of concentration of administrative and technological privileges for implementation in the individual processes of the organization. Specifically, it is proposed to include: Participates in the development and implementation of the cybersecurity policy; Projects future information systems capacity

requirements; Organizes the documentation of the processes and systems before the start of their operation; Offers a system of methods and tools for monitoring information systems; Participates in the maintenance of the digital infrastructure of the educational organization; Develops measures to increase the qualification of personnel involved in cyber security.

Results

The idea to create the current concept arose from constantly developing digitization processes in the public sector and business. These processes impose and require taking reciprocal measures to ensure data security in the organization. Along with the identified digitization trends, there is also a strong development in the regulatory framework for cyber security. For these reasons, the concept proposed above has been technologically realized and implemented in a real educational organization in the Republic of Bulgaria. For the period of implementation of the concept in the period 2022 – 2023, concrete results have been achieved in the direction of improving the cyber security of the organization. They are related to constant monitoring of the external perimeter of the organization, research and monitoring of user behavior and events in the organization, as well as introduction of specific control mechanisms.

The main results of the application of the proposed concept are presented in the following exposition according to the four layers defined above. The following elements are implemented for the first layer of the computer network. On the second layer of Endpoint protection, the implementation of ESET provides opportunities for active cyber protection of end devices. Figure 2 shows a screenshot from the ESET console, showing that the greater percentage of components included in the infrastructure are end-to-end.

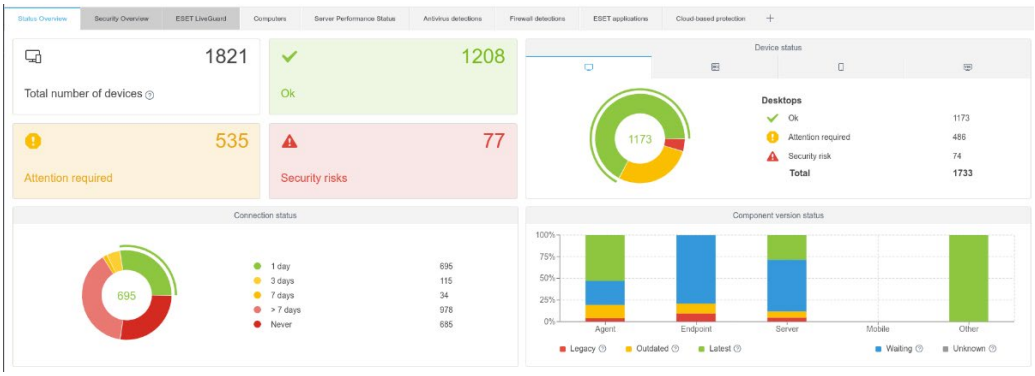


Figure 2. ESET console

In the organization, this refers to 1,208 out of a total of 1,821 devices. 1,173 out of 1,208 desktop computers are in OK status, which is 97.10% of all connected devices. Devices with the status "Security risks" represent 77 of the total 1,821 machines, which is just over 4% (Figure 3) (Table 1).

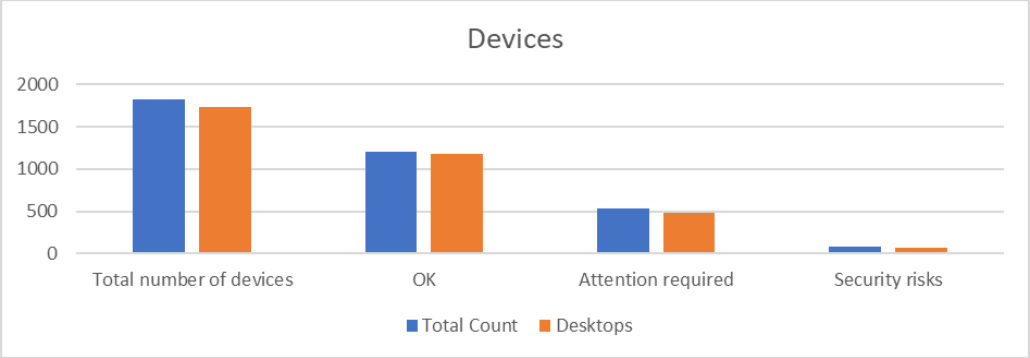


Figure 3. Devices by risk types

Table 1.
Devices by risk types

Devices	Total count	Desktops
Total number of devices	1821	1733
OK	1208	1173
Attention required	535	486
Security risks	77	74

The third layer of the proposed cyber security concept is the SIEM platform. The SIEM platform console provides very good capabilities for monitoring multiple events reported by end-point protection software. Specifically, Figure 4 shows administrator activity in active directory.

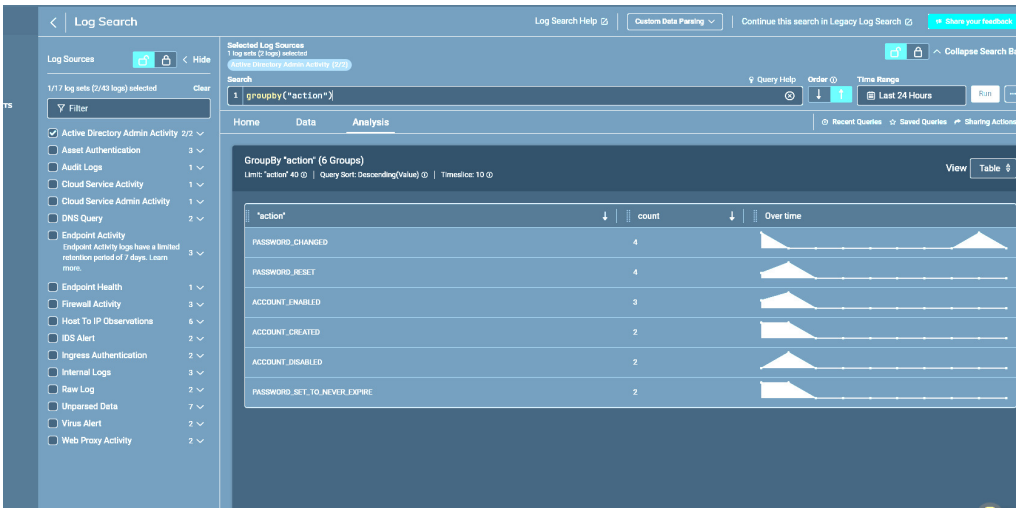


Figure 4. SIEM platform console

The actions observed are Password_changed, Password_reset, Password-enabled, Password_created, Password_disabled, Password_set_to_never_expire. Experimental data from her work are presented in Table 2.

Table 2.
SIEM platform console

Action	Count
Password_changed	4
Password_reset	7
Password-enabled	3
Password_created	2
Password_disabled	2
Password_set_to_never_expire	2

Figure 5 shows a screenshot of the Asset Discovery monitoring in the Security Operational Center, which represents the fourth layer of the proposed educational organization's cybersecurity concept. The figure shows the monitoring of accessed sites through the Information Asset Access Console. The main information provided to administrators is in terms of most seen asset types, most seen operating systems, most seen hardware, etc. There is a persistent trend towards a predominant connection to the monitored sites using the TCP protocol, much less activity using UDP, ICMP, etc.

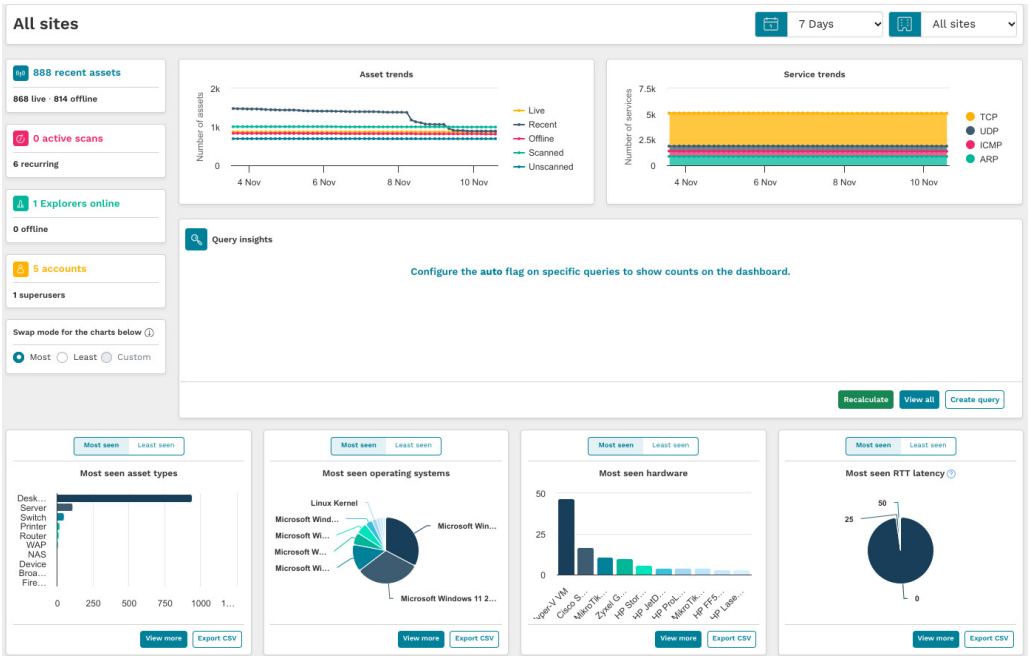


Figure 5. Asset Discovery

Of 74 monitored sites, through the Vulnerability Scan Monitoring of the Security Operational Center, the majority use Microsoft operating systems – 51 pcs., Ubuntu – 10 pcs., Linux – 8 pcs., Net Gear – 3 pcs., Unknown OS – 1 pc., Debian – 1 pc. (Figure 6). No vulnerabilities were found for the studied period.

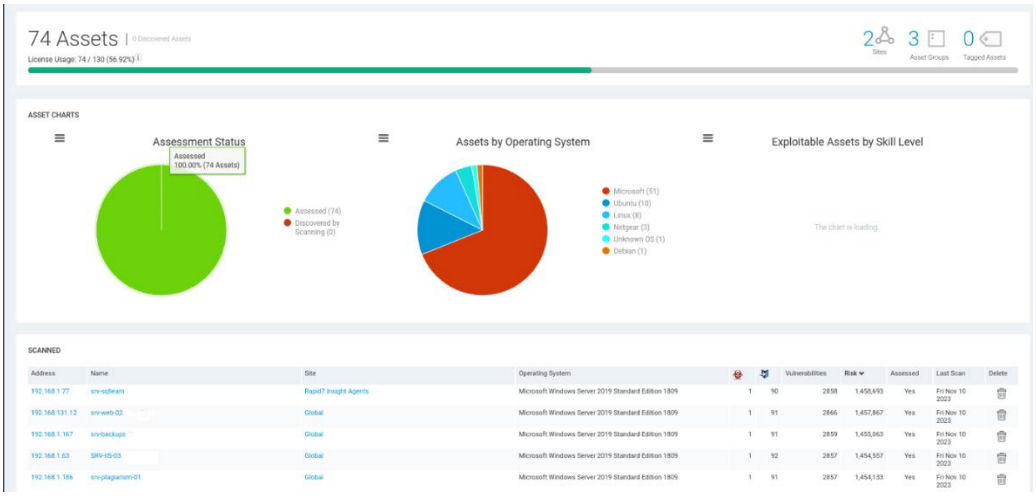


Figure 6. Vulnerability Scan

Risk assessment is an essential component of ensuring the cyber security of any organization. Cybersecurity strategies (Cheng, 2022) are being developed to address cybersecurity risks in educational organizations, with cybersecurity awareness (Khader, 2021) and risk identification (Ulven, 2021) playing an important role in this process. The risk assessment should be carried out, both in terms of the hardware resources and in terms of the developed software systems. This also applies to various tracking systems, such as those tracking the realization of graduate students (Kirilov, 2021). Risk assessment involves examining the likelihood or perceived frequency of an organization's cybersecurity negative event occurring. This includes a detailed assessment of the degree of significance of each of the identified risks and the likelihood of each of them occurring. In the specific educational organization, the risk assessment is carried out continuously over time. For each of the identified types of risk, the measures to reduce each of the risks should be determined. With this reduction, the risk factors are reduced to acceptable levels that guarantee data protection in the information infrastructure.

Another important component of organizations' cyber defense is constant monitoring of open infrastructure ports. To deal with cybercrime, it

is necessary for organizations to take adequate measures regardless of the type of cyber-attacks. Given the criticality of the information infrastructure, some measures are aimed at developing malware-resistant cyber-physical systems (Malik et al., 2023; Wai et al., 2023; Springer Link, 2023; Xun, 2023).

In a closed access cyberspace, it is important to analyze and evaluate not only remote access operations but also close access operations without underestimating the possible risk (Villalón-Huerta, 2023) to take adequate and situationally appropriate measures to prevent malicious actions.

Figure 7 shows a screen from External Attack Surface Monitoring. It shows information about Top Open Ports, Notable Ports, Top vulnerabilities, and Potential vulnerabilities. The monitoring does not show any problems with the external monitoring of the attacks. The data are listed in a Table 3.

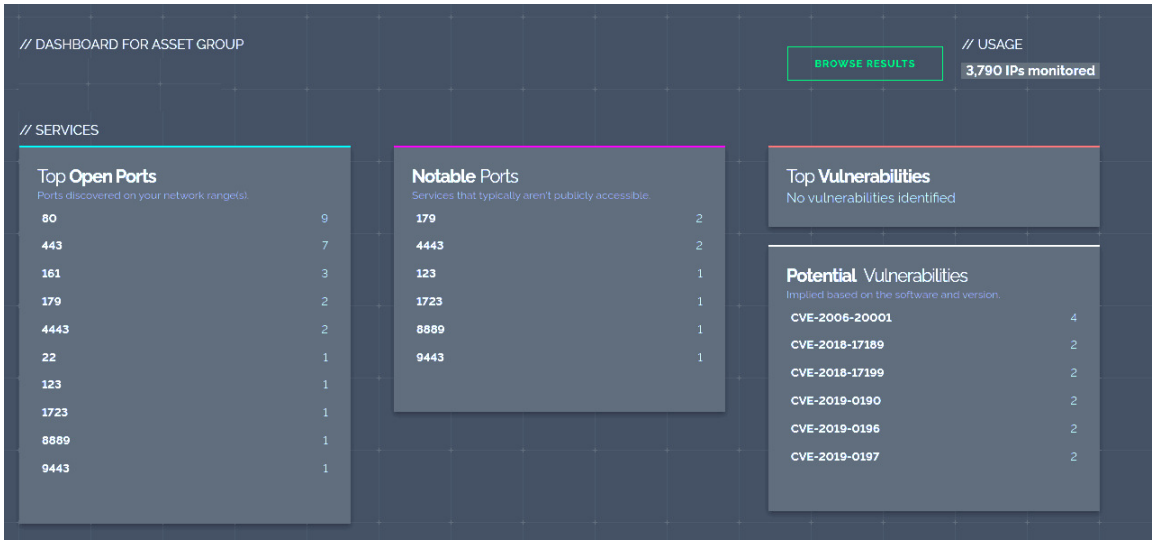


Figure 7. External Attack Surface Monitoring

Table 3.
External Attack Surface Monitoring and SIEM platform console

Open port	Count	Notable ports	Count
80	9	179	2
443	7	4443	2
161	3	123	1
179	2	1723	1
4443	2	8889	1
22	1	9443	1
123	1	-	-
1723	1	-	-
8889	1	-	-
9443	1	-	-

The external perimeter of the organization and its monitoring show opportunities to investigate and study the potential risks and threats of remote penetration of the organization's infrastructure. A specialized interface is provided for such monitoring in the Security Operational Center. Figure 8 shows a specific screen from the monitoring of the external perimeter of the educational organization.

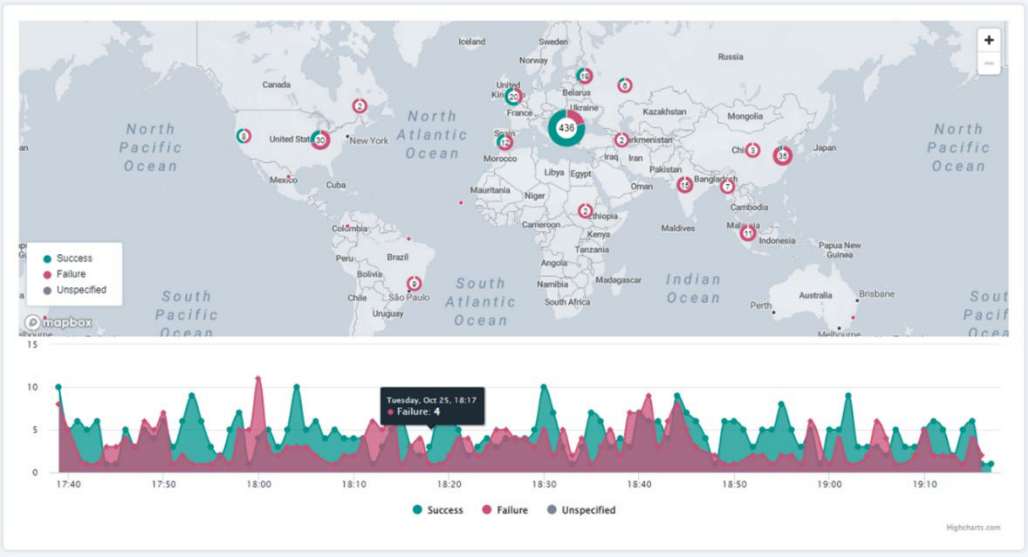


Figure 8. Management of the outer perimeter

It can monitor the successful and unsuccessful attempts to access the organization's information assets from different geographical points in the world. This analysis is a very essential component of detecting compromised user accounts that are activated from different points in the world at close points in time.

The presented results of implementation of the proposed cyber security concept clearly show that the proposed set of measures gives positive results. They are in the following directions: defined and maintained information assets, defined risk for each of the assets, comprehensive user behaviour monitoring on end devices, provided event management system, monitoring of the external perimeter of the organization, etc.

Discussion

A very essential component in providing an adequate cyber security concept for educational organizations is the analysis of the main processes that take place in the organization. This analysis is the basis for the application of various methodological components in the constructed security

concept. In this regard, literature does not offer a unified approach. Each organization should be perceived individually and according to its specifics. The question of the choice of specific technologies and tools to implement the individual layers of the concept is also worth discussing. Each software should be subjected to a careful comparative analysis. From it, it is important to derive the positive and negative sides of the analyzed platform. In some cases, it is also possible to carry out a preliminary assessment of the expected level of effectiveness of the platform, considering the specifics of the organization. The issue of the initial state of the baseline competencies of the organization's employees regarding cybersecurity is controversial. This issue requires careful planning of a set of employee training measures, both methodological and technological. The conducted research gives a positive answer and proves the thesis that adequate cyber security systems can be built and implemented in educational institutions, based on a set of organizational, technological and technical measures and control.

Conclusions

Cybersecurity is becoming an increasingly important factor in the success of organizations, both in the public and business sectors. Every organization should take protection measures that are adequate to the subject of activity and ongoing processes. In this context, it is important that the proposed technical, organizational and management aspects complement each other and bring a higher added value to the organization. Analyzing the characteristics of educational organizations and based on the experience gained from previous studies, the present study proposes a four-layer concept of cyber security. The concept has been applied and implemented in a specific educational organization, and all the results are summarized on this basis. They show that implementing such an approach ensures compliance with regulatory requirements and good practices in terms of providing an adequate level of cyber protection. The proposed cyber security concept has a marked geographic focus for countries with similar characteristics of educational organizations, such as those in the Republic of Bulgaria. The development of such an approach can be the basis for its adaptation in other organizations that have a similar subject of activity, as well as the development of scientific research in the field.

Funding

This research was funded by Project BG05M2OP001-2.016-0004-C01 "Economic Education in Bulgaria 2030", financed by Operational Program "Science and Education for Smart Growth", financed by the EU through low European structural and investment funds.

References

Alrubaiq, A., & Alharbi, T. (2021). Developing a cybersecurity framework for e-government project in the Kingdom of Saudi Arabia. *Journal of Cybersecurity and Privacy*, 1(2), pp.302-318.

Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information security and cybersecurity management: A case study with SMEs in Portugal. *Journal of Cybersecurity and Privacy*, 1(2), pp.219-238.

Bouramdane, A. A. (2023). Cyberattacks in Smart Grids: Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options, Including Ones That Incorporate Artificial Intelligence, Using an Analytical Hierarchy Process. *Journal of Cybersecurity and Privacy*, 3(4), pp. 662-705.

Capterra. (n.d.). Available online: https://www.capterra.com.

Cheng, E. C., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. *Information*, 13(4), 192.

ECS. (n.d.). *European Cyber Security Organization*. Available online: https://ecs-org.eu.

Enisa. (n.d.). Available online: https://www.enisa.europa.eu.

Eset. (n.d.). Available online: https://www.eset.com.

Eur-lex. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*. Available online: https://eur-lex.europa.eu/legal-content/bg/TXT/?uri=celex:32016R0679

Eur-lex. (2016). *Directive (eu) 2016/1148 of the european parliament and of the council*. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148.

Eur-lex. (2022). *Directive (eu) 2022/2555 of the european parliament and of the council*. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555.

Gartner. (n.d.). *ESET PROTECT Ratings Overview*. Available online: https://www.gartner.com/reviews/market/endpoint-protection-platforms/vendor/eset/product/eset-protect.

ISO. (n.d.). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection Information security management systems Requirements*. Available online: https://www.iso.org/standard/27001.

Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. *Information*, 12(10), 417.

Kirilov, R. (2020). Technological opportunities for the digitization of the career development processes. *Economic Alternatives*, (1), pp.184 -195. doi: 10.37075/EA.2020.1.10

Kirilov, R. (2021). Approaches for Building Information Systems for Monitoring the Realization of Students. *Economic Alternatives*, (3), pp. 469-481. doi:10.37075/EA.2021.3.09.

Majeed, A. (2023). Attribute-Centric and Synthetic Data Based Privacy Preserving Methods: A Systematic Review. *Journal of Cybersecurity and Privacy*, 3(3), pp.638-661.

Malik, M. I., Ibrahim, A., Hannay, P., & Sikos, L. F. (2023). Developing Resilient Cyber-Physical Systems: A Review of State-of-the-Art Malware Detection Approaches, Gaps, and Future Directions. *Computers*, 12(4), 79.

Milev, P. & Tabov, Y. (2022). Conceptual Approach for Presenting Text Data from Web-Based Information Systems in Structured Form. *Business Management* (1), pp. 50-64.

Mtc. goverment. (2019). *Naredba za minimalnite iziskvaniq za mrejova i informacionna sigurnost*. Available online: https://www.mtc.government.bg/sites/default/files/nar_minimalnite_izis kvaniq_mrejova_info_sigurnost-072019.pdf.

Rapid7. (n.d.). Available online: https://www.rapid7.com

Springer. (). *Call For Papers: Cyber Physical Systems and Industry 4.0: Security and Privacy Challenges and Solutions.* Available online: https://www.springer.com/journal/10207/updates/19086130.

Stone, M. (n.d.) *Cyber security in the public sector: Readiness and strategies*. Available online: https://www.verizon.com/business/resources/ articles/s/cyber-security-in-the-public-sector/

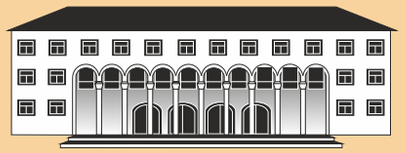
Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, 13(2), 39.

Villalón-Huerta, A., Ripoll-Ripoll, I., & Marco-Gisbert, H. (2023). A survey and characterization of Close Access Cyberspace Operations. *International Journal of Information Security*, pp.1-18.

Wai, E., & Lee, C. K. M. (2023). Seamless Industry 4.0 Integration: A Multilayered Cyber-Security Framework for Resilient SCADA Deployments in CPPS. *Applied Sciences*, 13(21), 12008.

Xun, P., Yang, Z., Zhu, H., & Tang, Z. (2023). Locating collaborative attack targets based on physical invariants toward cyber-physical systems. *International Journal of Information Security*, pp.1-19.

BUSINESS management



1/2024

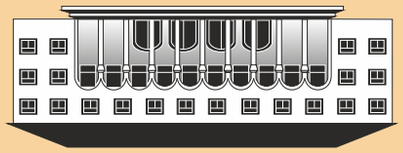
PUBLISHED BY
D. A. TSENOV ACADEMY
OF ECONOMICS - SVISHTOV

BUSINESS management 1/2024

ISSN 0861 - 6604
ISSN 2534 - 8396

БИЗНЕС управление 1/2024

ИЗДАНИЕ НА
СТОПАНСКА АКАДЕМИЯ
„Д. А. ЦЕНОВ“ - СВИЩОВ



Управление

БИЗНЕС

1/2024

The printing of the issue 1-2024 is funded with a grand from the Scientific Research Fund, Contract KP-06-NP5/42/30.11.2023 by the competition "Bulgarian Scientific Periodicals - 2024".

Submitted for publishinq on 22.03.2024, published on 23.03.2024,
format 70x100/16, total print 80

BUSINESS management

D. A. Tsenov Academy of Economics, Svishtov

Year XXXIV * Book 1, 2024

CONTENTS