TECHNICAL UNIVERSITY OF SOFIA

FACULTY OF MANAGEMENT

CENTRE FOR e-GOVERNANCE AT THE FACULTY OF MANAGEMENT

XV INTERNATIONAL SCIENTIFIC CONFERENCE "e-Governance and e-Communications" jointly with the "Science Days - 2023 " of TU-Sofia

June 2023
Sozopol
Bulgaria

ТЕХНИЧЕСКИ УНИВЕРСИТЕТ – СОФИЯ
Стопански факултет на ТУ - София
Министерство на електронното управление
Научно изследователски сектор при Технически университет - София
„Технически университет - София – Технологии“ ЕООД
Център за научни изследвания и обучение по е-Управление
към Стопански факултет на ТУ - София

TECHNICAL UNIVERSITY OF SOFIA
Faculty of Management of TU – Sofia
Ministry of e-Government
Scientific and Research Sector at the Technical University – Sofia
“Technical University - Sofia – Technologies” EOOD
Centre for scienticic research and education on e-Governance
at the Faculty of Management of TU – Sofia

XV МЕЖДУНАРОДНА НАУЧНА КОНФЕРЕНЦИЯ „е-УПРАВЛЕНИЕ И е-КОМУНИКАЦИИ“ в рамките на „Дни на науката – 2023“ на ТУ-София

XV INTERNATIONAL SCIENTIFIC CONFERENCE “e-Governance and e-Communications” jointly with the “Science Days – 2023” of TU-Sofia

СБОРНИК ТРУДОВЕ
CONFERENCE PROCEEDINGS

Юни 2023
Созопол
June 2023
Sozopol

Редакция от Международен Научен Комитет ♦ Edition by International Scientific Committee
Редактори: проф. д-р инж. Йорданка Ангелова, доц. д-р Светлана Борисова
♦ Editors: Prof. Dr. Eng. Yordanka Angelova, Assoc. Prof. Dr. Svetlana Borisova
Сътрудник оформление: Вл. Л. Станчев ♦ Associate layout: Vl. L. Stanchev

ISSN 2815-4525 (Online), **ISSN 2534-8523** (Print)

СЪДЪРЖАНИЕ ♦ CONTENTS with hyperlinks

Пленарен Доклад ♦ Plenary Report

Секция 1: „е-Управление и европейска е-Демократизация“
Section 1: “e-Governance and European e-Democratization”

РАЗВИТИЕ НА СИГУРНОСТА НА ERP СИСТЕМИТЕ

Ивелина Хинова
ТУ - София, България
ihinova@tu-sofia.bg

DEVELOPMENT OF ERP SYSTEM SECURITY

Ivelina Hinova
TU-Sofia, Bulgaria
ihinova@tu-sofia.bg

Abstract. In recent years, increased levels of threats to ERP systems have been detected. Therefore, additional tools related to the protection of business information are needed. These are complex solutions related to internal and external risks, maintenance, updating and data migrations for cloud ERP systems. Cyber defense is emerging as a specific IT skill focused on vulnerability understanding, appropriate response and centralized security monitoring. Security is an opportunity to upgrade ERP systems and establish modern security and integrity policies. In addition to the high degree of information, security of the system is the corporate administration of IT infrastructure.
Keywords: ERP, security, cyber-attack, audit, database, control, monitoring, authorization, password.

1. Introduction

Enterprise Resource Planning (ERP) systems allow better management of business processes, starting from human resources, marketing, customers, finance, accounting, warehouse, supply, projects and ending with production. They bring together all the assets of an enterprise in one unified application, with centralized business data. ERP systems contain critical data and important business information, therefore there is a risk and high danger of external interference. According to a number of recent studies, cyber-attacks are targeting ERP systems much more often, which affects the security of the company, because even if only a small part of the system is compromised by hackers, they will have access to a company's most valuable assets organization in all directions. Therefore, the security of ERP systems is the means that guarantees the safe operation of the company. In order to ensure the storage of the important business information, it is necessary to take measures to prevent intrusion into the database, which in practice is the protection of the ERP system.

The subject of the present study is the security of ERP systems, and the aim is to present the most effective methods of protection against cyber attacks used in practice.

2. Exhibition

The security of ERP systems covers security in areas such as: network infrastructure, operating system and database. This includes security for server

configuration, user registration and authorization, communication in the ERP system, and data integrity.

Implementation is by ensuring ERP system compliance with continuous monitoring, audits and security protocol including emergencies. With modern integrated information and communication systems, organized on a modular basis with interconnections between their constituent parts, providing comprehensive protection of ERP systems is a task with increased difficulty and a serious challenge for monitoring and maintenance.

2.1. Critical generalities

In a large company, with many users at different levels, with mobile applications, on a cloud platform, there are more opportunities for vulnerability in a system.ERP systems have a complex system configuration that allows system settings and user customization to be done very flexibly for users to perform their daily routine duties in the specific application, so there are hundreds of authorization objects in the systems.In cases where too many users have full rights and full access, this puts the ERP system exposed to cyber attack because there is a lack of strict requirements for authorization settings in ERP systems.

In the event of a failed system update, there is a possibility of potential violations. Password security of individual users is important for the security of the ERP system. Unfortunately, only 38%, according to the authors in (JSACPE 2022), of large organizations use multi-factor authentication as a means of protecting their users' accounts.

The chosen ERP platform provider, in most cases, offers a security solution that is often not integrated with cyber security, due to a lack of employees in the company who are not trained in system security management, which in turn further increases the possibility of internal and external malicious interference in the system.

2.2. Good practices

Timely control, through the implementation of ready-made ERP solutions for security, as well as their combination with other security operations, is of great importance in the implementation of cyber security of integrated information and communication systems in an organization. Communicating with employees at all levels about the potential risks to the reliability of the ERP system and training them to maintain its integrity is the guarantee of dealing with rapidly evolving threats and cyber security.

Risk of insider intervention, which is due to interference caused by a lack of awareness on the subject of cyber security, can be removed by rules and measures for safe passwords, which are associated with more frequent software and security updates to identify unauthorized access. This is one of the main requirements when checking the company's financial documents to establish the reliability of the data contained in them and their compliance with the current regulations.

Sensitive company data can be protected from internal and external intruders through strict and precise control of access to up-to-date information. Each company has its own cyber regulations, which are based on established best practices for protecting systems from cyber attacks, depending on the complex nature of the ERP system, such as size, component modules, and more. At different periods of time, it is imperative that these prescriptions be changed according to the given circumstances. Various authors (Balkan Services 2022, Charlie Hart 2021, Dragos 2020, ERP.bg

2023) have united on several basic activities that maximally protect the system from cyberattacks, because they allow to establish the interference and can recover the affected information.

2.2.1. Determining the information to be protected

It is necessary at an internal level in an organization to identify and locate the most important information, such as data and component modules. Consistently and systematically, it is necessary to evaluate the possible consequences of potential cyber attacks in these most important elements of the integrated information and communication system, regarding the bottom line for the company. What is the extent of damage, total and partial impact on the ERP system? What are the deviations from the normal operation of the ERP system, from time delays to data loss and network failure? Is it possible for routine operations to bypass the cyber attack? *For example: User information, according to the current GDPR regulation, should be defined as critical. The main elements, such as First Name, Surname, Family Name, Address, Email, Social Security Number, Telephone, appear in CRM, Billing, Delivery, Warranty and Post-Warranty Support, etc., so it is necessary to identify the interfaces that provide access to them.*

2.2.2. Road map to identify all interfaces with the system

In ERP systems, the flow of information is known. For security, it is necessary to prepare a Roadmap to identify all interfaces in the system and all interconnection points. From an IT management perspective, this is a difficult task and complex in terms of the system landscape. The identification of all ERP system interfaces with related information flows, through the roadmap, draws attention to those interfaces that are not needed because they are duplicated, little used, or inherited from other programs and can be reduced.

The creation of a roadmap depends on the volume of information and the components of the ERP systems. The process of defining and analyzing all the interfaces is long, according to the authors in (Federal Office for Information Security 2021) on the order of two months. Therefore, it is necessary to look at and study the traffic of a router-network to trace the interfaces. There are various examples of building a roadmap, for example by having a ring of firewalls around the ERP landscape with the sole purpose of reading the messages coming in and out and serving to detect data leakage.

Another option is to build digital twins by monitoring your own systems, which are used to optimize processes in ERP systems and also for cyber security purposes.

2.2.3. Middleware for monitoring data flows

A powerful security tool is the installation of middleware to which all established and recognized interfaces are redirected. In this way, the flow of data between the ERP system and the legacy environment is managed. The resulting middle layer of centralized system interfaces is convenient for monitoring and quick response when an interface is attacked.

The process of forwarding each interface connection to the middleware depends on the type and volume of data being transmitted. Managing the transition process on an interface-by-interface basis requires methodical and consistent tracking of each change.

2.2.4. Reduced vulnerability of data flows

With the introduction of middleware, risky interfaces begin to be systematically eliminated or improved. Certain interfaces become redundant and are not needed, so it is necessary to stop the flow of data flowing through them. This greatly reduces the number of points through which they can launch an attack.

When remediating risky interfaces, those interfaces that are easiest to remove for example, standard interfaces with data that do not need to be converted are addressed first, followed by complex interfaces.

A common practice in ERP systems is the file transfer protocol (FTP), which is convenient for hacking, as seen in Fig. 1. It is necessary to clean up acquired technologies to remove vulnerabilities to delay the possibility of external unwanted interference.

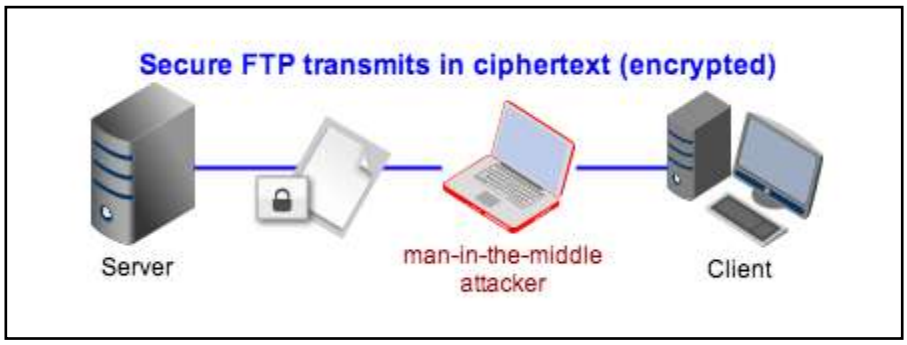


Fig.1 Secure FTP (JSACPE 2022)

A risk assessment is required for all interfaces that are difficult to migrate, which should consider how often they are used and what type of data they pass. After analyzing the risk situations, a certain interface can be removed or kept, but with additional monitoring.

2.2.5. Stop backing up "hacked" systems

A characteristic of ransomware, which prevents users from accessing their ERP system until a ransom is paid, is that it starts by encrypting backup data. This means that during the routine operation of the ERP system, already hacked data is archived, which leads to the rapid spread of infected data in the system.

Therefore, it is necessary to consider when to run backups daily or weekly. Having software available for daily network scans to detect ransomware increases the chance of spotting an attack. When a system is certified clean, it can be safely backed up and backed up. Nowadays, there are software for monitoring backup systems as well as for atypical backup activities that provide clues to a cyber attack.

The authors in (Balkan Services 2022) consider the example, as an alternative to real-time backup, of daily backup and saving a monthly historical image on a separate network. In this model, it is necessary to be able to recover a random sample of historical archive images, because if this is not achievable, it is imperative to formulate a concept to limit the data loss to a maximum of the time of the historical image - 30 days. This option is relatively expensive, but the information available in the system is very well protected.

2.2.6. The role of ERP system users and IT specialists.

Company employees directly involved in the operation of the ERP system at operational levels should be trained on how to react to cyber attacks. Their practical

experience should be used by cyber specialists to develop test situations related to real examples. The users of the individual modules, as part of the relevant business process, know in detail how the process proceeds, from the input data to the output product, and they can understand what the consequences of a cyber attack are. During the threat of external intervention, the joint work of the users of the ERP system and the IT specialists gives the sequence of actions, with the priority of a specific response. This ensures that responsiveness exercises are tested across end-to-end processes rather than isolated business data. As a result of the interaction of both parties, a protocol for neutralizing the cyber attack is documented.

2.2.7. A systematic approach to cyber-attack protection of ERP systems

In order to confirm the cyber security of the ERP system, it is necessary to methodically, systematically and consistently apply best practices established in practice. One of them is multi-factor authentication (MFA) and virtual private networks (VPN) to restrict user access, as seen in Fig. 2.

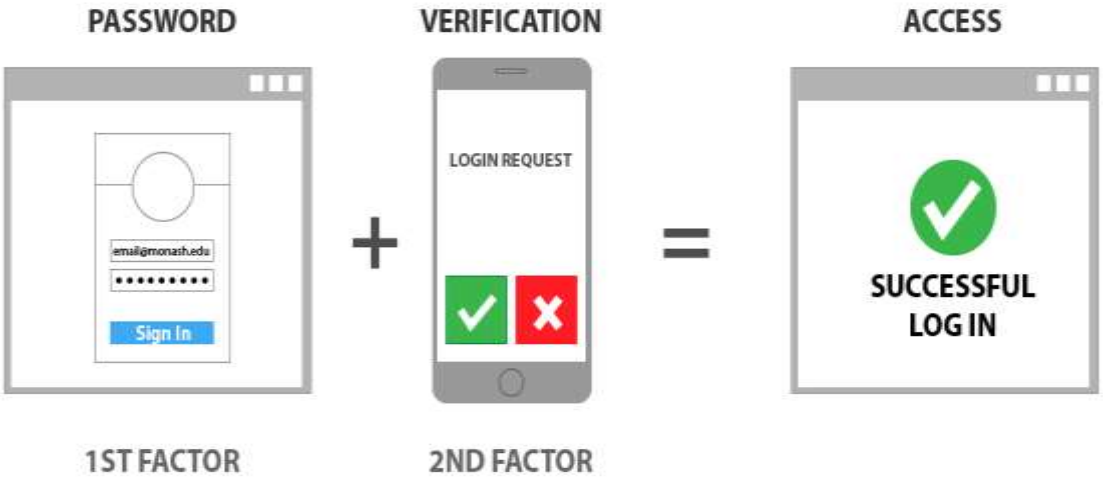


Fig. 2 MFA&VPN (MONASH University 2023)

In order to detect exploitation and fraud, regular vulnerability scans of the ERP system are performed to determine how long it takes to locate and neutralizing the threat. ERP systems contain large data sets, and automated scans are quite slow, so the best solution is to do this continuously for individual modules or parts of the system, scanning the flow of a specific business process.

2.2.8. Security as code (SaC)

Using security as code (SaC) is the most effective method, in terms of speed and quality, when securing cloud platforms, because the source code allows viewing how they work, detecting errors and other actions. SaC defines the programmatic standards for cybersecurity so that text settings files can be forwarded automatically. Therefore, the transfer of software to other computer platforms is carried out with source code. Infrastructure as code is the basis of security as code, evident from Fig.3.

Fig.3 Workflow of Infrastuctute as Code (Code Signing Store powered by digicert 2023)

For this reason, migrating data from ERP system applications to the cloud is an opportunity to modernize cybersecurity. Regardless of this fact, it is necessary to continue to correct local ERP systems and update their support in a timely manner.

3. Conclusion

In addition to internal risks, there are also external malicious intrusions, so it is necessary to use proven security practices for cyber protection of ERP systems.

ERP security solutions can monitor system settings, patch management, authorization, or RFC (Request for Comments) Internet standards for network communication as part of the modern computer industry for compliance. In order to implement effective protection of ERP systems, it is necessary to centralize security monitoring.The process of integrating local monitoring of ERP systems with fully focused professional external monitoring adds value to cyber security and IT operations in the system because such programs use UEBA (User Entity and Behavior Analytics) – to realize and understand the nature of deliberate actions in addition to rule-based monitoring. These additional tools enable continuous and automated audits that track IT environments from cloud applications to IT infrastructure and save time and money with out-of-the-box audit reports.

A comprehensive cybersecurity solution provides near-real-time monitoring of the ERP system. Due to the ongoing monitoring and available information about various events, it is possible to preserve the integrity of the data in the ERP system.

References

Balkan Services (2022). *Kakvo tryabva da znaete za ERP sistemite* [online]. Available from https://www.balkanservices.com/blog/kakvo-tryabva-da-znaete-za-erp-sistemite/[accessed: 07 July, 2022].

Charlie Hart (2021). *Troubling rise in supply chain cyber attacks. Supply Management* [online]. Available from:https://www.cips.org/supply-management/news/2021/april/troubling-rise-in-supply-chain-cyber-attacks/ [accessed 13 April 2021].

Code Signing Store powered by digicert. (2023). *What Is Security as Code & How Can I Implement It* [online]. Available from https://codesigningstore.com/what-is-security-as-code-how-to-implement-it [accessed May 2023].

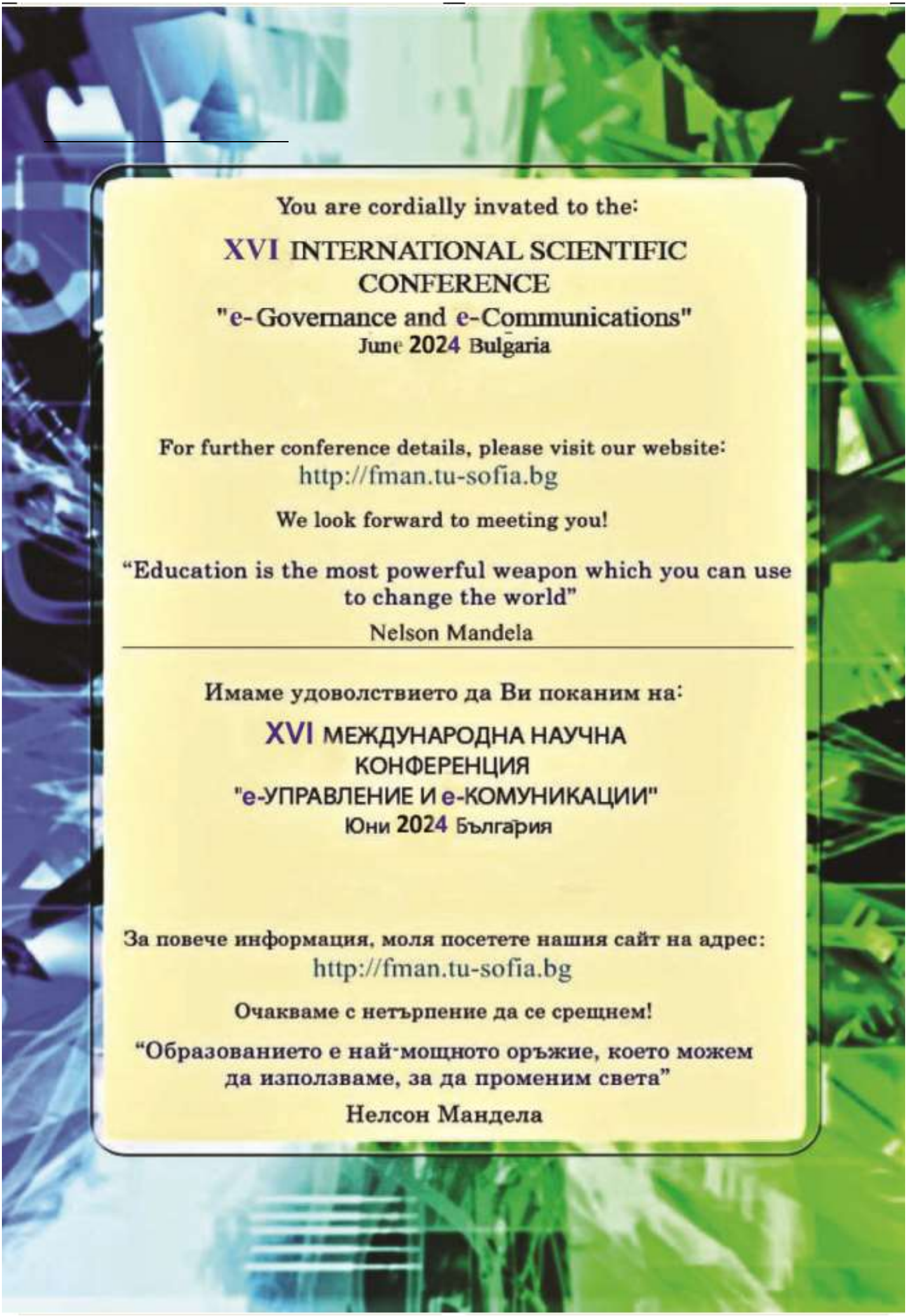
Dragos (2020). *Industrial Control Systems Cybersecurity year in review 2020* [online]. Available from: https://www.dragos.com/resource/dragos-releases-annual-industrial-control-systems-cybersecurity-2020-year-in-review-report/ [accessed February 2021].

ERP.bg (2023). *Kak da izberem ERP sistema* [online]. Available from https://erp.bg/information/how-to-choose-an-erp-system/ [accessed May 2023].

JSACPE/Words By John Carl Villanueva (2022).*What is Secure FTP & How Does It Work* [online] Available from https://www.jscape.com/blog/secure-ftp-simplified [accessed: December, 2022].

Federal Office for Information Security (2021). *IT-Security-Situation-in-Germany-2021*[online]. Availablefrom:https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2021.pdf?__blob=publicationFile&v=5 [accessed: October 2021].

MONASH University (2023). *Multi-factor authentication (MFA)* [online]. Available from https://www.monash.edu/esolutions/accounts-passwords/multi-factor-authentication[accessed: April 2023].



You are cordially invated to the:

XVI INTERNATIONAL SCIENTIFIC CONFERENCE

"e-Governance and e-Communications"

June 2024 Bulgaria

For further conference details, please visit our website:

http://fman.tu-sofia.bg

We look forward to meeting you!

"Education is the most powerful weapon which you can use to change the world"

Nelson Mandela

Имаме удоволствието да Ви поканим на:

XVI МЕЖДУНАРОДНА НАУЧНА КОНФЕРЕНЦИЯ

"e-УПРАВЛЕНИЕ И e-КОМУНИКАЦИИ"

Юни 2024 България

За повече информация, моля посетете нашия сайт на адрес:

http://fman.tu-sofia.bg

Очакваме с нетърпение да се срещнем!

"Образованието е най-мощното оръжие, което можем да използваме, за да променим света"

Нелсон Мандела