УДК 33:681.3(075)

ANALYSIS AND APPLICATIONS OF INFORMATION SECURITYIN CORPORATE INFORMATION SYSTEM, CLOUD COMPUTING AND BLOCKCHAIN

U.A. VISNIAKOU, HANI H.J. AL-MUSAWI, Z.R. AL-ATTAR ABDULRAOUF, R.KH. KHUDIER

Belarusian State University of Informatics and Radioelectronics, Republic of Belarus

Submitted24 March 2020

Abstract. The analysis of information security (IS) threats in the corporate information system(CIS), cloud computing environmentis executed. Separate approaches to the information protection in CIS, cloud environment, blockchain technology are considered. Separate applications for IS in CIS and cloud environments are presented. The blockchain application for use in education is considered.

Keywords: information security, CIS, cloud environment, blockchain, applications.

Introduction

Traditional information security (IS) tools, such as access control systems, firewalls, and intrusion detection systems, control only those information flows that pass through the channels intended for their transmission, so threats that are implemented through hidden information transmission channels cannot be blocked with their help. In these conditions, protection technologies against threats that are formed using hidden channels of information influence or within the security perimeter of a corporate computer network become important [1].

An important direction for improving security technologies and information security systems is to counteract bilateral threats, in which the subject and object of information interaction processes is a potential carrier of dangerous impacts. In such cases, it is necessary to use threat models that identify potential vulnerabilities both at the level of processes that control access to resources of guest operating systems (OS) or applications, and at the level of system calls to the hypervisor, which itself can become a source of destructive impacts that are implemented by disrupting the operation of the task scheduler or hardware Manager. The resulting threats must not only be detected quickly, but also block the used unauthorized channels of information impacts, which are implemented in cloud computing (CC) OV environment in a mode that is hidden for guest operating systems. Therefore, an important factor in improving the effectiveness of protection systems against hidden threats is taking into account the direction of transmission, syntax, and context of the transmitted data streams [1].

The development of CC technologies and environments introduces new sources of threats that must be taken into account when ensuring the security of computer systems and services. At the same time, the dynamic nature of information interaction processes makes it difficult to quickly assess the risks of violating the confidentiality, integrity, and availability of software and infrastructure resources provided in remote access mode.

Protection against such destructive impacts must be implemented at the level of system call management processes or control of undeclared capabilities (CUC) of application software, which requires the creation of new models and methods to counter attempts by both external and internal users to change the state of security of information resources in the environment of the CC.

Information security in corporate information systems

Development of the existing approach to the protection of CIS is more comprehensive and systematic view of the organization of protection by a decision task: choosing the means of protection

taking into account architectural and functional specificity of CIS, to focus on the security keys, and not on the threats; introduction to system protection the objective function, a measure of security; ensure and control the level of safety of the processes occurring in the keys; formalized representation of keys as an object of protection [2].

The task organizing the protection of information resources is formulated as the task of ensuring the safe functioning of automated business processes of the enterprise. Security as a quality is described by the properties of integrity (I), accessibility (A), confidentiality (C), etc., which can be set by linguistic values.

The main sources of information about the state of CIS elements that are important for the task of detecting attacks are identified: event logs and information about processes occurring on CIS servers, router logs, packets, transmitted over the network, event logs and information about processes occurring on workstations.

The model of multi-agent IDS is considered, which includes a set of interacting intelligent agents, information system components, and sources of information to be analyzed for the task of detecting attacks [3].

The structure of the protected network of the CIS is presented. The server is running Slack ware Linux 10.2 with the kernel version 2.4.31. This version of the kernel is the most researched, stable, and contains the minimum number of vulnerabilities detected. The server is protected using the IPTables firewall (v1.3.3). The result of combining IDS Snort and ITU IPTables is a two-level security system: at the first level, IPTables checks the incoming packet for compliance with its filtering rules, if the packet has received permission to pass through the firewall, it is checked by the intrusion detection system for the presence of malicious code in the body of the incoming packet.

Information security in cloud computing environment

The growth of threats calls for continuous improvement of approaches and methods for ensuring information security of the cloud computing environment (CCE), and the search for new technologies in the field of creating system of information security [4].

Traditional methods of intercepting system functions of guest operating systems do not allow detecting software "bookmarks" that are implemented in the OS at the boot stage. For example, the RuStock software agent can cause the system to fail and change pointers to system handler tables by accessing the structure of the processor's Executive region in the debugging session, and modify data from internal OS tables.

The following tasks are important for detecting malware in CCE [5]:

− development of a model of hidden threats to information security in the cloud computing environment, taking into account the active nature of subjects and objects of information interaction;

− development of a model of operations that occur with data when they are processed in the OV environment, which allows formalizing the description of information processes in the form of a multigraph of transactions;

− development of a method for detecting hidden threats using the proposed operation model based on the characterization of the transaction hierarchy;

− development and implementation of an algorithm for predictive identification of hidden threats based on the incident matrix and security policy rule tables in the guest OS and hypervisor;

The main security requirements for the CC environment are: round-the-clock security monitoring; detection of malware in guest NOS and hypervisor; protection of the VMS themselves; protection tools should not significantly affect the performance of the management subsystem. The solution for CCE providers to use specialized security tools that take into account virtualization technology; the integrity of data and applications; perimeter protection and delimitation of the network.

The main threats to the CC environment are: VMS are dynamic, they are cloned and can «move» between physical servers, which affects the development of security integrity; CC servers and local physical clusters use the same OS and applications, which increases the «attacked surface»; when the VM is turned off, it is at risk of infection; when using CC, the network perimeter is blurred or disappears, which leads to the fact that the protection of the less secure part of the network determines the overall level of security; to protect against functional attacks, the following security measures must

be used for each segment of the OV environment: for the domain controller server, effective protection against DoS attacks, for the Web server, page integrity control, for the application server, application-level screen, for the data storage system, backup, access control; most users connect to the cloud using the browser (Cross Site Scripting attacks, password theft, browser session hijacking, man-in-the-middle attacks, etc.).). A large number of VMS requires management systems that can be tampered with to block the operation of the VM; an attack on a hypervisor can lead to one VM being able to access the memory and resources of another.

Information security in blockchain and its application in education

The functioning of the block chain and its security is provided by miners and other block chain participants [6]. Access to the block chain takes place using special keys that guarantee the reliability of the entire network. Every user has it. A key is a set of cryptographic records. It is absolutely unique, which guarantees the impossibility of data substitution and hacker attacks. To do this, hackers need to access all the computers on the network. Mechanisms that ensure the efficiency and reliability of the block chain are algorithms of Proof of Work (PoW) − the work done, and Proof of Stake (PoS) − confirmation of the share. PoW in the block chain checks the calculations generated during the creation of a new block. The block is recognized as true and closed, provided that the value of its hash is less than the signature sought by miners. That is, a certain cryptographic cipher shows the authenticity of the block [7].

Confirmation of education documents is carried out using state registers, which is a complex and resource-intensive process. There is an increase in the number of forged documents in the world, which calls into question the effectiveness of modern mechanisms. Distributed Ledger technology (blockchain) is a sustainable technological trend that affects the development and quality of the digital economy. The existence of a mechanism for verifying the authenticity of educational documents that is resistant to malicious manipulation is an urgent task that goes beyond the sphere of education, possible solutions to which are proposed in this paper [8].

Current state. Educational institutions issue diplomas in paper form. Received diplomas on paper are subject to destruction in the event of natural disasters and falsification. It is necessary to define separate related sub-processes for an educational institution that determine the release of digital education documents using distributed registers (TRR) technology for storing digital «analogs» of documents. Determining an effective mechanism for verifying the authenticity of a document without the involvement of a third party. Advantages: reliability of storage, absence of intermediaries in the verification process, reliability of the received data.

Limitations. At the moment, there are three of them. There is no single digital document format, which can be solved within the framework of the Bologna process. The lack of productive information systems is that can ensure the execution of algorithms for issuing / checking in automatic mode. No legal basis for digital verification of authenticity without the participation of an authorized person-confirmation of educational documents is carried out by affixing an apostle on a copy or original of the document in accordance with the resolution of the Hague Convention of 1961.

The problem of validation. Transactions related to mechanisms for confirming authorship or authenticity using the digital equivalent of a document are used to present proof of one party to the other. The validator verifies the hash value, the transaction timestamp, and the identity of the bearer record. The mechanism for automated document validation based on the use of blockchain covers only two parties (the bearer and the verifier), which is not sufficient in the case of official documents, the issuer of which must be present in the model as a trusted third party. The confirmation model must establish not only that the document belongs to the issuer, but also confirm the issuer's authority to carry out this type of activity and additional information (for example, for the education sector, lists of training specialties for a certain period of time in accordance with the license).

Conclusion

1. The article considers the threats of is to the CIS, and suggests using the technology of multi-agent systems to protect the perimeter of the corporate system.

2. We consider the threats of is for the OV environment, and suggest using neural network technology to protect against malware that can be used in the SaaS model.

3. The mechanisms of blockchain technology with information protection through encryption and hashing of lists of distributed registers are considered. It is proposed to use this technology in education for document control.

References

1. Вишняков В.А. Информационная безопасность в корпоративных системах, электронной коммерции и облачных вычислениях: методы, модели, программно-аппаратные решения. Минск.: Бестпринт, 2016.
2. Visniakou U.A., Al-Musawi Hani H.J.//Reports of XVII Belorussian-Russian scien.-technic. conf. «Technical Tools of Information Defense». Minsk: BSUIR. 2019. P. 12.
3. Nikishova A.V. Multi-agent system for intrusion detection on enterprise information systems : abstract of PhD cand. tech. science : 05.13.19. Volgograd. 2013.
4. Visniakou U.A., Al-Attar Abdulraouf Z.R. // Reports of XVII Belorussian-Russian scien.-technic. conf. «Technical Tools of Information Defense» .Minsk.: BSUIR. 2019. P. 11.
5. Klementyev I.P. ,Ustinov. V.A. Introduction to cloud computing. Ulyanovsk.: UGU. 2009.
6. Swan M. Blockchain: a diagram of the new economy M.: Olimp-Business. 2017.
7. Visniakou U.A.,KhudierR.Kh.// Reports of XVII Belorussian-Russian scien.-technic. conf. «Technical Tools of Information Defense». Minsk.: BSUIR. 2019. P. 13.
8. Kachan D.A.// Digital transformation. 2018. № 5. P. 44–55.