METHODS FOR ENSURING INFORMATION SECURITY IN CLOUD INFRASTRUCTURES

O.Ch. Pardaev (Uzbekistan. Karshi branch of TUIT)

Abstract. *The article discusses the role cloud platform and ensuring information security of data in the cloud. The development of this technology in the field of cybersecurity is also promising.*

Keywords: *IaaS, SaaS, PaaS, Cybersecurity, information security confidentiality, cloud infrastructure, Indoor access to data, Intelligent.*

For each of the three models of cloud services has different types of threats.

• IaaS - Infrastructure as a Service

The vulnerability of this model lies in the isolation of different customers in the cloud, which provides virtualization technology.

In this case, virtualization should provide proper customer segmentation virtual machines located on the same physical entity as well as a need to protect against IP spoofing, and MAC address of the client, so that one client had no opportunity to take advantage of someone else's account.

• SaaS - Software as a Service

For this model, characterized by classic service for online application threats: XSS-vulnerability and vulnerabilities related to authentication (password leaks, etc.).

In this model, it must follow strict policies on identity management and access control applications.

• PaaS - Platform as a Service

Considering the cloud platform for application development, we must understand that the main problem for this model, as well as for IaaS, is to provide isolation of customers, as well as threats related to work through the programming

interface, ie, unreliable data encryption. In this case, it requires strong authentication to identify users, regular audit and confidentiality. It is understood that cloud solutions providers invest huge material and intellectual resources to ensure information security of data in the cloud, and the level of security in most cases is much higher than that, customers can provide their own means. Traditional methods of data protection are very often focused on building a centralized network and perimeter security tools such as firewalls and intrusion detection systems. This approach does not provide sufficient protection against attacks such as APT (advanced persistent threat), which are characterized by the fact that a hacker (often group) disguises its activity on the victim host under the daily operations, in connection with which it is difficult to detect.

Many companies also implement database auditing, access control to the directory (DAP - Directory Access Protocol) and systems for the analysis of incoming information from third-party systems (SIEM - Security Information and Event Management) to gather information about the operation and processes, but monitoring and correlation events by themselves do not provide information security data.

It is important to provide comprehensive protection, which must first include an early warning system for the beginning of the attack, displaying suspicious incoming requests, detailed analytics continuous incoming data, etc. You must also provide data encryption; however, here it is important not to lose sight of the weaknesses: the encryption keys, access control, monitoring and data access. If the encryption keys are not adequately protected, they are vulnerable to theft, if keys are well protected, but not access control is reliable enough, it is possible to gain access to sensitive data, "posing" an authorized user. Encryption must be implemented on the basis of reliable key management solutions available to ensure guaranteed protection keys. Encryption works in conjunction with other data protection technologies, and provides additional information about security for the construction of a comprehensive multi-layered approach to the protection and confidentiality of data and reduce the risk of breaking in the cloud and beyond.

The specifics of computer networks, in terms of their vulnerability, mainly associated with the presence of an intense information exchange between geographically dispersed and diverse (heterogeneous) elements.

Vulnerable are literally all the main structural and functional elements of the CS: workstations, servers (Host-machine), bridging (gateways, switching centers), communication channels, etc.

Thus, an effective solution to information security cloud infrastructure shall include:

• Indoor access to data

It is necessary to ensure reliable control of the encryption keys.

• Access policies

Only authorized users have access to confidential information.

• Intelligent

The system should collect information for the analysis of user behavior and alert if it detects suspicious activity. Information security in the cloud is not a trivial task, however, with an appropriate approach, you get a perfect balance of all the advantages of the cloud model and the high level of protection, security and availability of your data and information systems. The best option when customers use each individual virtual machine (VirtualMachine - VM) and virtual network. Separation between VM and consequently between the users, provides hypervisor. Virtual networks, in turn, deployed using standard technologies such as VLAN (VirtualLocalAreaNetwork), VPLS (VirtualPrivateLANService) and VPN (VirtualPrivateNetwork). Some providers put data of all clients in a single software environment, and due to changes in its code trying to isolate customer data from each other. This approach is reckless and unreliable. First, the attacker may be able to find a gap in the non-standard code that will allow him to gain access to data that he should not see. Secondly, the error code may cause one customer accidentally "see" other data. Recently, there were also those other cases. Therefore, to distinguish between the use of user data of different virtual machines and virtual networks is a smart move.

Depending on the jurisdiction, laws and regulations and any special provisions may vary. For example, they may prohibit the export of data, require the use of well-defined measures of protection, the availability of compatibility with certain standards and availability of audit. Ultimately, they may require that, if necessary, access to the information could be government agencies and the courts. Neglect provider to these points may cause its customers to substantial costs due to legal implications.

The provider is obliged to follow strict rules and stick to a single strategy in the legal and regulatory spheres. This concerns the security of user data, their exports, compliance, audit, security and deleting data, as well as disclosure of information (the latter is especially true when a single physical server can store multiple clients). To find out, customers are urged to seek professional help, which will study the matter thoroughly. Therefore, service providers are required to adhere to certain rules of conduct in the event of unforeseen circumstances. These rules should be documented. Providers must focus on identifying incidents and minimize their effects, informing users about the current situation. Ideally, they should regularly provide customers with maximum detail information on the issue. In addition, customers themselves have to assess the likelihood of problems related to security, and to take the necessary measures. Despite the fact that today we have a much wider range of tools for security than ever before, the work is far from over. Intrinsically safe data (self-protecteddata) - is the encrypted data, which is integrated in the security mechanism. This mechanism includes a set of rules, which may or may not meet the environment in which the data are intrinsically safe. When you try to access the data, the mechanism of checks on the safety of the environment and open them only if the environment is safe.

Trusted Monitor (trustedmonitor) - this software is installed on the server cloud computing provider. It allows you to observe the actions of the provider and transmit the results to the user, who can ensure that the company operates in accordance with the regulations.

References:

1. Fundamentals of Information Security. Textbook for high schools / EB Belov, VP Moose, RV Meshcheryakov AA Shelupanov. -M.: 2006 - 544

2. Vikhorev SV Kobtsev RY How to determine the sources of threats? // Open systems №7-8 / 2002. http://www.elvis.ru/files/howto.pdf.

3. GOST R ISO / IEC 17799-2005.

4. ISO / IEC 17799: 2000 (BS 7799-1: 2000).

5. Orifjon, P. (2023). INFORMATION SECURITY CLOUD INFRASTRUCTURE. *Innovations in Technology and Science Education*, *2*(11), 43-45.

6. Uzakov, O. S., Raxmatullayev, D. A., Bekmatov, A. K., & Dilmurodov, Z. D. (2023). IOT TEXNOLIGIYALARI XAVFSIZLIGIDA SMART HOUSELARNI MOBIL QURILMALAR YORDAMIDA BOSHQARISH. ОБРАЗОВАНИЕ НАУКА И ИННОВАЦИОННЫЕ ИДЕИ В МИРЕ, 23(7), 105-107

7. Бекматов, А. К., Кутдусова, Э. Р., Мукимов, Ш. И., & Давлатова, Н. Н. (2023). ПРОГРЕССИВНЫЕ ТЕНДЕНЦИИ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Экономика и социум, (6-1 (109)), 1264-1270.