Ella FIK[1]

Supervisor: Ivan TYSHYK[2]

DOI: https://doi.org/10.53052/9788366249844.07

BEZPIECZNE PLANOWANIE ZASOBÓW PRZEDSIĘBIORSTWA

Streszczenie: W artykule przedstawiono uporządkowany obraz wszystkich mechanizmów zapewniających bezpieczeństwo informacji w systemach zarządzania przedsiębiorstwem. Uwzględniono podstawowe aspekty bezpieczeństwa pracy z systemami realizującymi strategię ERP, bezpieczeństwo sieciowe systemów ERP, a także bezpieczeństwo na poziomie bazy danych, serwera aplikacji oraz użytkownika reprezentatywnego.

Słowa kluczowe: planowanie zasobów przedsiębiorstwa; analiza systemu i rozwój programu; Internetowy serwer transakcji; Bezpieczna komunikacja sieciowa; Kontrola dostępu oparta na rolach; autonomiczne miejsce pracy.

SECURE PLANNING OF ENTERPRISE RESOURCES

Abstract: This article gives a structured view of all the mechanisms for ensuring information security in enterprise management systems. The basic aspects of security while working with systems that implement the ERP strategy, network security of ERP systems, as well as security at the database, application server's and representative user's levels are considered.

Keywords: Enterprise Resource Planning; system analysis and program development; Internet Transaction Server; Secure Network Communications; Role-Based Access Control; autonomous workplace

[1] Lviv Polytechnic National University, Department of Information Security, speciality: Cyber security

[2] PhD, Lviv Polytechnic National University, Associated Professor of Department of Information Security, ivan_tysh@i.ua

1. Introduction

The theory of professional communication claims that every organization has many external and internal connections, which form its “nervous system” and determine how effectively it will function. Indeed, the company's chances to succeed are directly related to how quickly and accurately information is transmitted - not only to the outside (to counterparties or customers), but also inside, between departments and branches.

A small enterprise can manage business processes “manually” because it is easy to exchange data on a small scale. However, as the company grows, maintaining communication becomes more difficult, and the logical question of calling for help from information technology arises. Some are researching themselves using a program that is self-contained or upgrading their own CMS server or accounting software; some are using existing decisions..

A popular option for such a turnkey solution is an ERP system that turns individual elements of a company into a integral organism. Production, finance, warehouses, personnel - all this becomes part of a single information network and thus gets the opportunity to interact with each other without errors and malfunctions. However, any such structure has its own vulnerabilities, and therefore, it must be protected from threats [1].

The company's information infrastructure is a large and complicated complex, an important component of which is the integrated enterprise information resource management system (ERP system). Elements of an ERP system contain information critical for the organization’s activities, the confidentiality and safety of which is of great importance. That is why every link in the ERP system must be reliably protected, since negative external or internal impact on any part of it can have the most serious consequences for the performance of the entire organization.

To create a secure information space within the enterprise, there are complex, infrastructure-integrated solutions proposed to protect the ERP system from external and internal infringements. Given the nature of modern threats, remedies have been built based on a practical approach which focuses on anticipating them rather than dealing with the consequences [2].

2. Analysis of research and publications

The Positive Technologies study shows that 94% of IT systems are not protected by hacking. The most common vulnerabilities on the network perimeter are Internet-based interfaces for managing network equipment, servers, and the use of vocabulary passwords, including the default password set.

When testing against an intruder (for example, a regular employee located in a user-defined network segment), in all cases, unauthorized privileged access to critical resources (banking, ERP systems, and other key components of the network) can be obtained. In 78% of cases the internal violator can get full control over the information infrastructure of the organization.

The most widespread vulnerability of internal network resources remains weak passwords. At the same time, each system detects simple administrator passwords (up to 6 characters long). The next most common of the vulnerability of internal networks - an insufficient level of protection of privileged user accounts (for 88% of systems).

In 50% of cases, there is the use of outdated software, which allows you to exploit such vulnerabilities as Heartbleed and Shellshock [3].
Contrary to the widespread opinion that the main danger to the company is the external intruders, operating on the Internet, the so-called hackers, the real threat to the modern company comes from internal intruders. According to numerous studies, more than 70-80% of all violations in the corporate environment account for the proportion of internal intruders [4].
An internal intruder is a legitimate employee of an organization that has some access to its information resources. Moreover, the causes of breaches into organization may be both staff misconduct or intentional actions on their part. So, according to world statistics, the proportion of internal intruders which intentionally commit unlawful acts, accounting for about 20% of all incidents in the company, while external intruders are guilty of only 5% of similar cases [5].
E-mail remains an important tool for cybercriminals, but they are experimenting with new methods of attack through mobile devices and social networks to reach a larger audience with less power.
"Over the last year, 70% of cases of social network fraud were hand-crafted, because intruders used the willingness of people to trust the content they share with their friends" (data from the Symantec report).
While fraud through social networks allows cybercriminals to be enriched quickly, some rely on more profitable and aggressive methods of attack, such as extortion programs, whose numbers are increasing significantly from year to year.
For today, Pancreas (Ransomware) is one of the most active classes of malware. In recent years, programs-extortion have evolved and from a simple lock screen with the requirement of redemption have gone to more dangerous actions.
Now the basis of the Ransomware class are so-called encryptors. These are Trojans that, without the user's knowledge, encrypt their data, including personal photos, archives, documents, databases, drawings - in short, everything that represents the value of the victim. The decryption of these files requires victim to pay, and sometimes a lot of money. The most notable examples of such encryption are CryptoLocker, CryptoDefence (and its successor, CryptoWall), ACCDFISA, Gpcode.

3. Network security of ERP-system

Integrated ERP system security covers a number of objects, solving for each of them a number of security-related tasks: protection against external and internal threats, protection of servers and users of the ERP-system, trust building system, protection of network connections. Moreover, to ensure comprehensive protection of the system, the blocks of the complex must interact and complement each other, and this is possible only if all of the protection components are functioning.(fig.1)

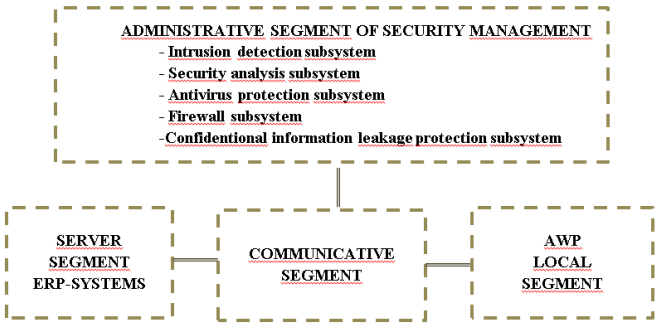

Figure 1. Protection complex structure of ERP-system

To ensure information security in ERP-systems, in addition to standard information security tools, additional software tools, including cryptographic ones, are used to fulfill all information security requirements [4]. In SAP, passwordless authentication and encryption of communication channels is implemented using the SNC (Secure Network Communications) mechanism for exchanging data via the DIAG protocol, and SSL / TLS protocol for exchanging data via HTTP / FTP [6]. The vendor provides SNC support for inter-server communication, and also, on the terms of additional licensing, means of limited SNC support for client PCs (SAP NetWeaver Single-Sign-On).

4. ERP database security

One of the most important components of an ERP system is the database. The database for the ERP system can be placed on the same physical server as the application server, but, as a rule, one or several separate servers are allocated for the database. It is advisable to programmatically and physically isolate these servers from the rest of the company's computer infrastructure. It is recommended to strictly restrict access to physical servers and hardware components. For example, database server equipment and network devices should be located in closed guarded premises. Access to backup media should also be limited. The operating system under which the DBMS of the ERP system runs must also be configured so that access to the database is open only to the application server. No user of the ERP system should have direct access to the database.

Data processing occurs on the application server, and thereby it provides user authorization, as in it prohibits or allows access to various objects of the ERP system. Most modern ERP systems use the RBAC (Role-Based Access Control, role-based access control) model to allow users to perform only strictly defined transactions and access only certain business objects. In the RBAC model, decisions to grant user access are made based on the functions that the user performs in the organization.

A role can be understood as the set of transactions that a user or a group of users can perform in an organization. A transaction is some procedure of converting data in a system, plus data on which this procedure can be performed. Each role corresponds to many users who belong to this role. A user can have several roles. One of the advantages of the RBAC model is the ease of administration.

The role assigned to the user consists of a set of privileges, and it is the presence of the necessary privileges that the server checks during the execution of the transaction. Thus, the presence of authority allows you to achieve the necessary level of detail in access control. It should be noted that the necessary roles and the corresponding powers should be based on a clearly defined organizational structure and business processes that the company seeks to automate through the introduction of an ERP system. Therefore, data about the organizational structure should be available prior to designing a set of necessary roles for users.

The last line of information protection is the actual user's workplace, that is, the client computer. Statistics say that most IT crimes are committed by the employees of the company, and not by external attackers. The first bottleneck is the user's login into the system. The traditional approach assumes that the user has a name and password for entering the OS and other name and password for entering the ERP system. This approach has many disadvantages. An alternative to the traditional approach can be user authentication using digital certificates, especially since PKI-based mechanisms are found in most modern ERP systems. Accordingly, it is possible to achieve, among other things, the implementation of the Single Sign On concept. The concept of Single Sign On implies that a user passes the authentication procedure only once to enter various information systems.

To protect I/O devices, there are various additional software tools installed directly on the client computer. To provide protection against information leakage through various channels, special leak prevention systems are used.

Conclusion

It has been established that the complexity of an ERP system leads to the emergence of its vulnerabilities. ERP systems process a large number of different transactions and implement complex mechanisms that provide different levels of access for different users. Practically for any ERP, in addition to the standard means of information protection, as a rule, additional software tools, including cryptographic ones, and the involvement of third-party suppliers are required to fulfill all information security requirements. The security mechanisms listed above should form the basis of the ERP security system. These tools provide protection at the level of individual components of the ERP system. As a rule, security systems entail a high project cost and low productivity. Such contradictions always exist. A balance must be struck between security, performance and usability.

REFERENCES

1. NIKOLAJ GOLOVKO Ensuring the security of SAP ERP systems using the example of the SafeERP Suite solution – Access mode: *https://www.anti-malware.ru/practice/methods/security-of-erpsystems-on-example-safeerp-suite*
2. WEI SHE & BHAVANI THURAISINGHAM Security for Enterprise Resource Planning Systems – Access mode: *https://www.tandfonline.com/doi/abs/10.1080/10658980701401959*
3. Positive Research 2015. – Access mode:

http://www.ptsecurity.ru/download/PT_Positive_Research_2015_RU_web.pdf
4. Symantec. Internet Security Threat Report (April 2015 Volume 20 v2). – Access mode: *http://www.symantec.com/security_response/publications*.
5. FELTUS C., PETIT M., SLOMAN M. Enhancement of Business IT Alignment by Including Responsibility Components in RBAC // Proceedings of the CAiSE. Workshop Business/IT Alignment and Interoperability (BUSITAL2010). 2010. Vol. 599. Pp. 61-75.
6. BULDAKOVA TATIANA, ALEXEY KORSHUNOV. Security information security ERP systems – Access mode: *http://www.arbornetworks.com/news-and-events/press-releases*.