UDC 004.4

O.V. GALOCHKIN, D.I. UHRYN, A.V. HOSTYUK, O.G. USHENKO

COMPLEX PROTECTION OF INFORMATION IN OPERATING SYSTEMS

Yuriy Fedkovych Chernivtsi National University
Kotsyubynsky 2, Chernivtsi, Ukraine, e-mail: o.galochkin@chnu.edu.ua

Анотація. Безпека даних – одна з головних завдань, що вирішуються IT-відділами компаній. Причому мова йде не тільки про запобігання витоку корпоративної інформації, зниження обсягів паразитного трафіку і відбитті атак на ресурси компанії, але і про оптимізацію роботи системи в цілому. Знайти універсальне рішення в даному питанні практично неможливо: неоднорідність сфер діяльності і структур організацій переводить завдання в категорію, яка потребує індивідуального підходу. У статті розглянуто основні інформаційні загрози корпоративних систем, а також методи захисту від поширених загроз і атак на інформаційні системи підприємства, оцінено вартість конкретних рішень.

Ключові слова: інформаційні системи, безпека даних, захист інформації, програмне забезпечення, брандмауер, антивірусні системи.

Abstract. Data security is one of the main tasks solved by IT departments of companies. Moreover, it is not only about preventing the leakage of corporate information, reducing the volume of parasitic traffic and repelling attacks on the company's resources, but also about optimizing the system as a whole.

It is virtually impossible to find a universal solution in this matter: the heterogeneity of the spheres of activity and the structures of organizations translates the task into a category that requires an individual approach. The article deals with the main information threats of corporate systems, as well as methods of protection against common threats and attacks on information systems of the enterprise, estimated the cost of specific solutions.

KeyWords: information systems, data security, information protection, malware, firewall, antivirus systems.

DOI: 10.31649/1681-7893-2022-44-2-44-48

INTRODUCTION

Information security is relevant for corporations with a collapsible, territorially divided, rich structure: great banks, transnational and state-owned companies. The most common corporate measures of similar organizations were inspired by different generations and different manufacturers, which significantly simplifies the process of managing the IT system. In addition, the information structures of corporations vary widely, stench is formed from different databases, sets of different subdivision systems and tasks of a local nature.

SETTING TARGETS

To rob the resources of corporate peers is especially discriminating. In the process of exchanging data between the organizations and the middle ground, they can be attacked by malware, like destroying the database and making the transfer of data to third persons. So, the task of information security is relevant for medium and small businesses. Especially today, if business processes are actively moving to the virtual space: payment for goods and services via the Internet, e-mail, IP-telephony, cold stores, virtual servers - everything has become typical for today's mid-Lanka companies, as well as hacker attacks, data, including financial ones.

1. CORPORATE SECURITY THREATS

The most serious concern for IT infrastructure today is viruses, spyware and adware, spam, and phishing attacks such as “in-service” attacks, on the main side of the Internet resource and social media. There are three main types of threats to security information systems (IS) [1]:

- threats of violation of confidentiality of information;
- threatening damage to the integrity of information;
- threaten the disruption of the system's performance (visiting the service).

Threats of violating confidentiality are aimed at disclosing confidential and secret information. With the implementation of these threats, information becomes available to individuals, as if they were not guilty of the mother, access to it. In terms of computer security, the threat of breach of confidentiality is more likely to occur if unauthorized access to certain sensitive information that is stored in a computer system is removed from one computer system to another.

Threaten the destruction of the integrity of the information that is stored in the computer system and is transmitted over the communication channel, aimed at changing the quality of the creation, which will lead to the destruction of the quality of the total collapse. The integrity of the information can be destroyed on purpose by the evildoer, and also as a result of the influx of the outer environment that drains the system. This threat is especially relevant for information transmission systems - computer networks and telecommunication systems. Special damage to the integrity of information is not a trace of a rogue with a sanctioned snake, as it is created by important persons with a primed method.

Threaten the disruption of serviceability (in service) aimed at creating such situations, if they do special actions or reduce the efficiency of IC, or block access to resources. For example, if one user of the system is trying to try to take access to the current service, and the other one is blocking that access, then the first user will be denied access to the service. Blocking access to a resource can be permanently temporary [1].

Moreover, as a threat, they can be as well as external users and company employees (often hatefully). The implementation of harmful algorithms can lead to paralysis of the system and failures, and to waste, control, or leak of information. This can lead to time and financial expenses for the company. In this rank, the main tasks of the information security system are:

- ensuring the availability of data for authorized correspondents - the possibility of prompt withdrawal of information services;
- guarantee of the integrity of information - relevance and security in the event of unauthorized its changes or degradation;
- ensuring the confidentiality of statements.

For the purpose of achieving the goals, such methods of protection of information, such as registration and protocol, identification and authentication, access control, creation of firewalls and cryptography are being developed [2].

It is important to note that the nutrition of information security is assessed and on the state level and is known in such laws of Ukraine: “On the basis of national security of Ukraine” [3], “On the concept of national program informatization” [4], “On national program” [4], as well as the Strategy of National Security of Ukraine, as approved by the Decree of the President [6].

The advances of requirements are hanging up to the defense of the tributes in the computer nets:

- selection of licensed technical documents and software;
- re-verification of the objects of information for compliance with regulatory protection measures;
- compiling a list of acceptable use of software and prohibition for use outside of this list
- use and timely updating antivirus programs, conducting regular checks of computers on the subject of malware infection;
- development of methods for prevention of how to prevent the consumption of viruses in the net;
- development of methods for recovering and updating infected software.

In banking structures, it is also necessary to secure access to data in order to intimidate evil spirits from the side of employees and to implement methods of encrypting data with the method of ensuring the security of electronic penny transactions.

2. COMPLEX DATA SECURITY IN CASE OF AN INDEPENDENT SYSTEM AND INFORMATION SECURITY AND PROTECTION OF INFORMATION

The latter protection of information can only secure a complex data, which allows one-hour use of hardware, software and cryptographic benefits (necessary additional security).

A similar approach transmits analysis and optimization of the entire system, and not just a few parts, which allows you to ensure a balance of characteristics, although it is not uncommon to increase some parameters to improve others.

The standard for the security system is ISO / IEC 17799 [7], which conveys an integrated approach to the completion of the tasks set. Compliance with this standard allows you to vary the level of security of confidentiality, integrity, reliability and availability of data.

Organizations come in, who get used to a complex approach, as an independent tool and unite all methods, like victorious, into a single wholesome mechanism. Such a child will ensure the safety of data at all stages of their processing. When properly organized, the system does not create serious incompatibilities in the process of work [8, 9, 10].

A comprehensive analysis includes a detailed analysis of the implementation of the system, the assessment of security threats, the prevention of damages, which are victorious in the event of a system, and those capabilities, the analysis of the response of internal and external threats, and the assessment of the possibility of making changes to the system [11, 12].

3. METHODS AND GETTING INFORMATION PROTECTION

- shaping the security policy and folding the relevant documents;
- promotion of defense technical aids.

Although more efforts for more security are in great companies is aimed at implementation of the first paragraph, the other is not less, but maybe more, important. The main hardware and software features are:

Firewalls

The stench will take care of the measure and protect the damage by the users of the established safety rules. Modern firewalls are breathtaking with manual controls and great functionality (the ability to organize VPN, integration with antiviruses, etc.). Now, there are trends:

- before the implementation of firewalls by hardware rather than software (it allows you to reduce the cost of additional possession and components, software and increase the levels of protection);
- to the delivery of personal firewalls;
- to focus on the SOHO segment, to expand the functionality of these kits.

Antivirus protection of information.

Efforts of the largest selections of directing for the security of the echelon defense of corporate measures [8]. Systems, as they grow, protect robotic stations, as well as block mail gateways, proxy servers and other ways of virus penetration. An effective solution to this problem is parallel use of two or more antiviruses, in which various methods are implemented detection of malicious software.

Intrusion Detection System (IDS).

Similar systems are tightly integrated with the help of blocking high-speed spills and with protection analysis systems. The system of correlation under accentuates the respect of the administrator only on those subs, as they can manage the real infrastructure of the company. IDS manufacturers tend to increasing their speed indicators development.

Access control and protection of information in the middle of the border.

With the method of ensuring data security, great companies carry out automation of the management of information security and the creation of a central management console, as well as demarcation of access between employees due to their functionality. In the field of creating virtual private networks (Virtual Private Network - VPN), it is necessary to improve the efficiency of encryption processes and ensure the mobility of clients (to access to the data with any attachment). The distributors of control systems instead of trying to ensure that the systems they create do not create discomfort for the users.

4. VARIETY OF SOLUTIONS TO THE PROTECTION OF INFORMATION

Complex protection of the protection of information changes from time to time and is assigned to us in front of current economic minds and present threats. Thus, the increase in the number of malware attacks and the economic crisis will stop the world's companies and power structures from choosing only really practical solutions. This explains the change of orientations. Whereas earlier corporations were targeted in the first place at the highest levels of the sovereigns, they were able to defend information, now it is no less important to ensure the real security of the business through the provision of reliable software and hardware facilities.

More and more companies are pragmatically integrating their own work with other IT structures, security systems, Security information and event management (SIEM) systems, so that they can provide real-time analysis of security measures that appear in the form of outbuildings and add-ons. SIEM is represented by add-ons, accessories or services, and it is also used to save data and generate stars with a method of wisdom with other business data.

The function of administrating the protection of the defense is transferred to the security department in ITTV. The cores of the companies and IT directors attach special respect to the manufacturability of the using, the wisdom and the ceremoniality of the defense. There is a transition from a simple sense of inconsistency (a purely technical approach) to a risk-correcting management (to a complex approach).

All the more important for customers are the soundness of the sound, the clarity of the interface, the security of the virtual environment when working with mobile devices. In connection with the increase in the number of targeted attacks, the growth will affect solutions in the field of protection of critical objects and infrastructure (investigation of computer incidents, the prevention of DDoS attacks).

The cost of organizing a corporate system for the protection of information is based on an impersonal warehouse. In particular, it's out to lie in the sphere of activity of the company, the number of employees and users, the territorial distribution of the system, the necessary level of protection, too. On the cost of the work, the price of the attached installation and software, the cost of the work, the availability of additional services and other factors are added.

For example, the cost of the Cisco Web Security hardware and software system varies from $170 to $2370 in terms of the number of cases [9]. Add McAfee Web Gateway, which is deployed locally, to secure a web host with a high level of speed action, ranging from $2,000 to $27,000. There are two options for spitting: in front of a hardware annex and in front of a virtual machine [10].

Websense

Web Filter subdivides websites into non-specific (over 100) categories, and at the same time allows you to win the Internet in the open world with the method of business development [11]. The number of users can vary from 250 to 250 thousand people with the possibility of their interaction in the border. The Websense Web Filter program is designed to work with the wired infrastructure components and secure the highest level of flexibility and control when working in the web space. The price of the Websense Web Security web filter can reach $40,000. Barracuda Web Filter is an advanced integration solution for blocking add-ons, content filtering and protecting against malicious software, suitable for businesses of any kind. It uses flexible security policies for blocking unwanted websites and Internet applications, visiting which interferes with business [12]. Also Barracuda Web Filter will block spyware programs and other forms of malicious software in your business. The Barracuda Web Filter service starts at $1500 for a fee, serving up to 100 customers at once (a machine for servicing 300-8000 customers costs $4000). Under the Tsomu Shorichna, the onset of the SOFTWARE is about $ 400-1100.

CONCLUSION

The company's current information security is based on the concept of a comprehensive protection of information, which can simultaneously develop a variety of mutually compatible software and hardware solutions and approaches of a social nature, as they support and supplement one another. In the rest of the hour, there was a trend towards the creation of universal rich-tasking products. However, whether a universal software is made up of a number of add-on modules, directing to "close" specific problems of information security. Some of them are fighting against spam and phishing, others are focused on monitoring IT infrastructure and scams, and others are controlling the editing of fax alerts and the flow of information through external storage, archiving and encrypting documents. Call the software product lists to give you the opportunity to choose and compile decals of mutual IT solutions in a group, depending on the company's current tasks, which allows you to manage your budget wisely.

REFERENCES

1. A. Yu. Shcheglov. Protection of computer information from unauthorized access / A. Yu. Shcheglov. - St. Petersburg. : Science and technology, 2004. - 384 p.
2. V.L. Ortinsky. help / [V.L. Ortinsky, I.S. Kernitsky, Z.B. Zhivko, M.I. Kernitska, M.O. Zhivko]. - Kyiv: Low unity, 2009. - 541 p.
3. About the foundations of national security of Ukraine: Law of Ukraine of December 19, 2003 No. 964-IV // Information of the Supreme Council of Ukraine. - 2003. - No. 39. - Art. 351.
4. About the concept of national informatization programs: Law of Ukraine dated February 4, 1998 No. 75/98-VR // Information of the Supreme Council of Ukraine. - 1998. - No. 27-28. - Art. 182.
5. About the national program of informatization: Law of Ukraine dated February 4, 1998 No. 74/98-VR // Information of the Supreme Council of Ukraine. - 1998. - No. 27-28. - Art. 181.
6. About the National Security Strategy of Ukraine: Decree of the President of Ukraine dated February 12, 2007 No. 105/200 // Official Bulletin of Ukraine. - 2007. - No. 11. - Art. 389.
7. Tom Carlson Information Security Management: Understanding ISO 17799. [Electronic resource]. – Access mode: http://www.kwesthuba.co.za/downloads/ 03_ins_info_security_iso_17799_1101.pdf

8. Eric Byres. Layered defense against cyber threats. [Electronic resource]. – Access mode: http://ua.automation.com / content/jeshelonirovannaja-oborona-vs-kiberugrozy
9. Cisco Products & Services. [Electronic resource]. – Access mode: https://www.cisco.com/c/en/us/products/index.html
10. McAfee Web Gateway. [Electronic resource]. – Access mode: https://www.mcafee.com/en/resources/datasheets/ds-web-gateway.pdf
11. Websense Web Filter. [Electronic resource]. – Access mode: http://www.infobezpeka.com/products/trafic/Webse nse_Web_Filter/
12. Barracuda Web Security Gateway. [Electronic resource]. – Access mode: https://spro.com.ua/products/barracudanetworks/barracuda-web-filter

Надійшла до редакції 15.10.2022р.

GALOCHKIN OLEKSANDR – Ph.D, Assistant Professor of Computer Science Department, Yuriy Fedkovich Chernivtsi National University, Chernivtsi, Ukraine, ***e-mail:* *o.galochkin@chnu.edu.ua***

UHRYN DMYTRO – D.Sc. (Tech), Assistant Professor of Computer Science Department, Yuriy Fedkovich Chernivtsi National University, Chernivtsi, Ukraine, ***e-mail: d.ugryn@chnu.edu.ua***

HOSTYUK ARTUR – student of Computer Science Department, Yuriy Fedkovich Chernivtsi National University, Chernivtsi, Ukraine, ***e-mail: hostiuk.artur@chnu.edu.ua***

USHENKO OLEXANDER – D.Sc., Professor, Head of Optics and Publishing Department, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine, ***e-mail:* *o.ushenko@chnu.edu.ua***