Analysis of information security issues in corporate computer networks

E A Lavrov, A L Zolkin, T G Aygumov, M S Chistyakov and I V Akhmetov

1 Computer science department, Sumy State University, Rymskogo-Korsakova Street 2, Sumy 40007, Ukraine
2 Computer and Information Sciences Department, Povolzhskiy State University of Telecommunications and Informatics, L.Tolstogo Street 23, Samara 443010, Russia
3 Department of computer engineering software and automated systems, Dagestan State Technical University, I. Shamyl Street 70, Makhachkala 367000, Russia
4 Economics and finances department, Financial University under the Government of the Russian Federation (Vladimir branch), Tikhonravova st., 1, Vladimir 600037, Russia
5 Department of digital technologies and modeling, Ufa State Petroleum Technological University, Kosmonavtov Street 1, Ufa 450062, Russia

E-mail: prof_lavrov@mail.ru

Abstract. This article discusses the main problems associated with information security in corporate networks and ensuring the reliable operation of information systems and the services they provide. Information security is understood as the security of information resources and information systems, as well as the supporting infrastructure from accidental or deliberate influences of a natural or artificial nature, fraught with harm to the owners or users of information resources. Currently, there are major changes in information security issues. They relate to the methods of work of attackers, the conditions of crimes committed in the computer sphere, as well as the consequences of illegal activities.

1. Rationale
The question of assessing and accounting for the value of circulating information flows is arising during building the complex corporate information security systems. In modern information theory, the concept of the value of information (as well as the concept of information itself) is not strictly and formally defined. Due to this fact it makes it difficult to determine the levels of necessary and sufficient protection mechanisms. In reality, to achieve the greatest efficiency, the means of protection must adequately protect information, in accordance with its value in the corporation [1].

Insufficient knowledge of the issues of quantitative assessment of the value of information in modern science does not make it possible to assess and justify the necessary costs for building protection systems for information and telecommunication systems, the justified moments of their application and the composition of protective functions.

Security is a buzzword today. The significant changes over the past decade can be noted considering the solution to the problem of protecting access to corporate network resources in development. In the late 1980s, the physical vulnerabilities of the system and threats of physical access of unauthorized
persons to the system were the most worried issues. Therefore, the decisions were mainly related to organizational measures. By the mid-90s, the emphasis have shifted. A strong influence was exerted by connection of the corporate network to the Internet and by building distributed networks (connection of networks of the company's branches to the head corporate network) as well as the danger associated with computer viruses. During this period, computer security of the corporate network ceased to be determined only by the correctness of job descriptions and the "strength of the door" in the room with servers and was mainly transferred to the management of the company's IT personnel [2]. The scheme for solving these problems in most cases consisted in finding and detecting system vulnerabilities, and then in eliminating the found "gaps". Therefore, various network scanners and security scanners, systems for auditing events and its subsequent analysis have become greatly important. Companies have provided the maximum protection of the perimeter of their network from unauthorized access by random persons, real hackers and computer viruses that penetrated the network along with corporate mail or from the Internet. Since the late 90s, information security solutions have shifted from search and elimination of security gaps to the risk management. Vulnerabilities and risks are analyzed for each information system, while active network control is strengthened and various incidents are continuously investigated. It is on these approaches that modern network security systems are based [2].

2. Security issues of the modern corporate networks

New information technologies are being actively introduced into all spheres of the national economy. The emergence of local and global data transmission networks provided computer users with new opportunities for the rapid exchange of information. Until recently such networks were created only for specific and narrowly focused purposes (academic networks, networks of military departments, etc.). Now the development of the Internet and similar systems led to the use of global data transmission networks in the daily life of almost every person [1]. With the development and complication of means, methods and forms of automation of information processing processes, the dependence of society on the degree of security of the information technologies used by it increases.

A corporate information system is a complex structure that combines various services necessary for the functioning of a company. This structure is constantly changing (new elements appear, configuration of existing ones changes). As the system grows, ensuring information security and protecting business-critical assets becomes more complex.

Today, corporate computer networks play an important role in the activities of many organizations. E-commerce is increasingly turning from an abstract concept into reality. Most corporate networks are connected to the global Internet. If earlier the Internet has united a small number of people who trusted each other, now the number of its users is steadily growing and already amounts to hundreds of millions. Due to this fact the threat of external interference in the normal functioning of corporate networks and unauthorized access to their resources by intruders - the so-called "hackers" [3] is becoming more serious.

The Internet is based on the standards of IP networks. In such a network each device is uniquely identified by its unique IP address. However, during interaction in an IP network, we cannot be absolutely sure of the authenticity of the unit (the subscriber with whom the exchange of information is carried out), which has a specific IP address. It is due to the fact that programming tools allow manipulating the addresses of the sender and recipient of network packets, and this fact is already part of the problem of ensuring the security of modern network information technologies.

By connecting to public networks, the organization pursues certain goals and tries to effectively solve the following tasks [3]:

- provide internal users with access to external resources. First of all these resources are WWW - resources, FTP - archives, etc.;
- provide access to users from the external network to some internal resources (corporate WEB-server, FTP-server, etc.);
- ensure interaction with remote branches and departments;
• organize access to the resources of the internal network of mobile users.

In solving these problems, the organization is faced with a number of security problems. During interaction with remote branches and mobile users through open channels, there is a threat of interception of transmitted information. Providing universal access to internal resources creates the threat of external intrusions aimed at obtaining confidential information or disabling the internal network units.

Investments of organizations in ensuring information security in the form of purchased means of protection, cost of remunerating specialists, costs for external security audit, etc., are steadily increased from year to year but often do not pay off. This happens mainly due to the fact that the most organizations continue to adhere to a fragmented approach, which is justified only with a weak dependence of the organization on information technology and a low level of information security risks [4]. An adequate level of information security can only be provided by an integrated approach, which implies the systematic use of both software, hardware and organizational protection measures on a single conceptual basis. In this case, organizational measures play a primary role. The most sophisticated and costly security mechanisms are ineffective if users ignore basic password policy rules, and network administrators violate established procedures for granting access to corporate network resources.

3. Current trends in the development of malicious software

The rapid development of communications and information technologies determines the main trends in the development of malicious software. Malicious software is a collective term for malware or code that can harm a computer system.

Malicious software is deliberately designed to be hostile, intrusive and aggressive. It tries to penetrate the system, inflict damage, partially take over control of some processes, or completely disable computers, computer systems, networks, tablet and mobile devices. Like the human flu virus, it interferes with normal functioning.

The purpose of malicious software is to generate illegal profit at the expense of the user. Despite the fact that the malware cannot damage system hardware or network equipment, it can steal, encrypt, or delete data, alter computer functions, or take control of it. In addition, it can monitor computer activity without the user's knowledge.

Viruses are already very rare. They are completely replaced by all kinds of network worms and spyware. Today a dozen file viruses that remain active and even sometimes show the bursts of activity can be counted. These bursts are related to the side effect of these recent viruses reflected in infection of executable files with mail worms. These files send themselves along with e-mails infected with the worms. Very often, there are occurrences of the Mydoom, NetSky or Bagle mail worms infected with file viruses such as Funlove, Xorala, Parite or Spaces [5].

The main and dominant representatives of modern viruses are network worms, which actively use all kinds of technologies of classic viruses.

Everything is very simple, with the advent of the Internet, networking and communication technologies received a strong impetus in their development. The volume of information transmitted through all kinds of communication channels has increased greatly over the past few years, and will continue to grow in the future. All this creates a favorable environment for the rapid development of malicious programs, especially against the background of poor security of most of the networks. Virus writers are actively looking for all kinds of vulnerabilities in software and system software, which are then used for network attacks and the introduction of viruses.

Next, we will consider the main characteristic features that have most clearly manifested themselves in recent years in modern viruses [5]:

• active use of all kinds of vulnerabilities in various operating systems and software;
• use of spam technologies allows the rapid spread of viruses throughout the Internet;
• use in one virus: stealth, polymorphic, trojan, backdoor technologies;
• creation of a gigantic network of "zombie machines" allowing for massive DDoS attacks and sending out copies of the virus;
• sending messages by e-mail in order to attract users to infected sites;
• actual separation of Trojan proxy servers into a separate class, closely related to sending spam;
• use of backdoors and vulnerabilities left by other worms for spreading (the Mydoom.a worm);
• sending itself in the form of archives (Bagle, NetSky);
• sending itself in the form of password-protected archives with the password in the text of the letter or in the form of a picture (Bagle);
• refusal to send its' body by e-mail and instead of it sending a link in the letter to a website or to a previously infected computer (NetSky);
• active use of social engineering.

The category of network worms includes programs that distribute copies of themselves over local and/or global networks in order to [6]:

• penetration to remote computers;
• launching of its' copy on a remote computer;
• further distribution to other computers on the network.

To spread, worms use a variety of computer and mobile networks: e-mail, file-sharing systems, and instant messaging systems.

Most of the known worms spread in the form of files: an attachment to an email, a link to an infected file on some web or FTP resource, a file in the exchange directory, etc.

Some worms (the so-called bodyless or package worms) spread in the form of network packages, penetrate directly into the computer's memory and activate their code.

To infiltrate remote computers and launch their copy, worms use various methods: social engineering (for example, the text of an e-mail that calls to open an attached file), gaps in the network configuration (for example, copying to a disk with a full access), errors in security services of operating systems and applications.

The category of classic computer viruses includes programs that distribute copies of themselves over the resources of a local computer for the following purposes:

• for subsequently launch of its code upon any user actions;
• for its' further implementation in other computer resources.

Unlike worms, viruses do not use network services to infiltrate other computers. A copy of a virus reaches remote computers only if the infected object is activated on another computer for some reason that does not depend on the functionality of the virus, for example [6]:

• during infecting the available disks, the virus penetrated files located on a network share;
• the virus has copied itself to removable media or it has infected files on it;
• a user sent an email with an infected attachment.

Trojan horse software includes soft that carry out various actions that are not authorized by the user: collecting information and transmitting it to an attacker, destroying it or maliciously modifying it, disrupting the computer's performance, or using computer resources for unseemly purposes.

The category of hacker utilities includes:

• utilities for automation of creation of viruses, worms and Trojan horse soft (constructors);
• software libraries designed to create malicious software;
• hacker utilities for hiding the code of infected files from anti-virus scanning (file encryptors);
• Utilities that play "dirty tricks" with a computer. These type of utilities makes it difficult to work with a computer;
• software that informs the user on knowingly false information about its actions in the system;
• other programs that intentionally cause direct or indirect damage to computers (both local and remote).

The analysis of the classification of malicious software has revealed the presence of a huge number of various programs of this kind with classification features. Each malicious software, in its turn, has different functions, tasks and properties. The implementation of information security threats associated with the use of malicious software can lead to a violation of all information security properties (confidentiality, availability and integrity). At the same time, the number of malicious software grows as the software develops and becomes more complex, and the interactions leading to the implementation of such threats are rather complex.

4. Findings
Aside the intensive development of computer facilities and information technologies, the vulnerability of modern information systems and computer networks, unfortunately, does not decrease. Therefore, the problems of ensuring information security attract close attention of both specialists in the field of computer systems and networks, and numerous users, including companies working in the field of electronic business [7,8].

Ensuring the security of the corporate information system is a priority task for the company's management, since the promptness of decision-making and the efficiency of the company largely depend on the preservation of confidentiality, integrity and availability of corporate information resources [9,10].

Despite the good awareness of company leaders about the risks to which information security is exposed by employees of their organizations, they do not take adequate measures. Companies continue to focus on external threats such as viruses, while the severity of internal threats is continually underestimated. Companies willingly go to the procurement of technical equipment, but are not ready to classify personnel problems as a priority [4].

Software shall not have any gaps and IT managers must incentivize vendors to deliver reliable software, or security costs will rise. Businesses should require confirmation that the software they buy is secure and that the manufacturer has reviewed the code for security reasons.

References
[1] Biyachuev T A eds. L G Osovetvskiy 2004 Corporate networks safety (St. Petersburg: Saint Petersburg ITMO University) p 161
[2] Afanasev A Corporate network safety: protection from within https://www.aladdin-rd.ru/company/pressroom/articles/bezopasnost_korporativnoj_seti_zasita_iznutri Accessed on: 08.11.2020
[3] Course for Information Technologies Safety http://asher.ru/security/book/its/23 Accessed on: 08.11.2020
[4] Issues of informational safety in the Internet http://itzashita.ru/lekcii/problemy-informacionnoj-bezopasnosti-v-internet.html Accessed on: 08.11.2020
[5] Trends of development of the modern malicious software http://whatis.ru/razn/razn24.shtml Accessed on: 08.11.2020
[6] Malware (malicious) https://www.tadviser.ru Accessed on: 08.11.2020
[7] Sokolov A V and Shangin V F 2002 Information protection in distributed corporate networks and systems (Moscow: DMK Press publisher) p 656
[8] Riakhovskii A N, Zheltov S I, Kniaz' V A and Iumashev A V 2000 A hardware and software complex for producing 3D models of the teeth 79(3) 41-5
[9] Utyuzh A S, Yumashev A V and Mikhailova M V 2016 Spectrographic analysis of titanium alloys
in prosthetic dentistry *Journal of Global Pharma Technology* 8(12) 7-11

[10] Utjuzh A S, Yumashev A V and Lushkov R M 2016 Clinical example of orthopedic treatment of a patient after mandible resection caused by sarcoma with the use of dental implants *Clinical Dentistry* 4 56-8