УДК 621.396

НЕКОТОРЫЕ ОСОБЕННОСТИ АТАК В КОМПЬЮТЕРНЫХ СЕТЯХ

© 2022 Ю. П. Преображенский, Е. Жуков, Е. Г. Завгородний

Воронежский институт высоких технологий (Воронеж, Россия)

В работе обсуждаются некоторые особенности атак в компьютерных сетях. Показаны примеры возможных уязвимостей.

Ключевые слова: компьютерная сеть, атака, защита информации, уязвимость.

The development of modern information technologies leads to a gradual transition to the integration of autonomous computers and local networks into a single corporate network of the organization. In addition to the obvious advantages, such a transition also brings with it a number of problems specific to corporate networks [1]. These problems are faced by both security specialists and employees of automation departments. The reasons for these problems include:

- The complexity and heterogeneity of the software and hardware used. At the moment, it is very difficult to find networks built on the basis of only one network operating system (OS). Experience shows that in Russian organizations the following variant of building a corporate network is used: workstations running Windows.

- A large number of corporate network nodes, their territorial distribution and lack of time to control all settings. It is no longer a rarity when nodes united into a corporate network are scattered across different territories of not only one city [2], but also a region. This feature, as well as the lack of time to control all settings, does not allow administrators to personally and timely control the activities of system users on all nodes of the corporate network and the compliance of software and hardware settings with specified values.

- Connecting the corporate network to the global Internet and access of external users (customers, partners, etc.) to the corporate network [3]. This reason leads to the fact that it is often very difficult to determine the boundaries of the network and all users connected to it, which can lead to attempts of unauthorized access to protected information [4].

One of the important problems arising from the above reasons is the increase in the number of corporate network vulnerabilities. Therefore, to eliminate them and ensure an appropriate level of protection of information circulating in the corporate network [5], various mechanisms and security tools are used. The appropriate setting of these tools depends on the information processing technology adopted in the organization, the procedure and rules for handling protected information. The collection of such rules, laws and practical recommendations for ensuring security, covering all the features of the information processing process, is called a security policy [6]. Firewalls, intrusion detection systems, traffic encryption systems, "mobile code" control systems (Java, ActiveX), etc. can be referred to the means that ensure the security policy and, accordingly, the protection of information processing technology [7].

These days, attacks on computer networks such as "denial of service "(DoS, Denial of Service) are the most common attacks. The purpose of such attacks is to bring the server (the object to which the attack is directed) into a state where it cannot respond to client requests. A side effect of such attacks is that there is a lot of traffic directed towards the target of the attack. With the help of this attack, the largest and most famous companies, such as Yahoo!, eBay, Buy.com, Amazon.com, CNN.com and a number of lesser known ones, have been disabled for a long time.

The main feature of a DoS attack is that there is no computer [8] that is too powerful for

Преображенский Юрий Петрович – Воронежский институт высоких технологий, канд. техн. н., профессор, e-mail: petrovich@vivt.ru.

Жуков Евгений – ВИВТ-АНОО ВО, студент, e-mail: chup_yulliya90@yandex.ru.

Завгородний Евгений Германович Воронежский институт высоких технологий, студент, e-mail: chup_yulliya90@yandex.ru.

it. For a server of any capacity, you can always select the required number of computers participating in the attack, which will disable the attacked server with their packets. It should also be noted that most Internet worms that spread their bodies via e-mail are also a DoS attack that disables mail servers [9].

Examples are the Morisson worm and the Melissa virus, which indicate that you can disable a mail server of any power.

The second feature of a DoS attack is the extremely difficult localization of attackers. In addition to the fact that the attack comes from many addresses (which makes it difficult to counter by simply blocking traffic outgoing from these addresses), these addresses may well belong to unsuspecting users. An attacker can only be traced by a message about the start of an attack, and the path of this message is not so easy to trace.

Finally, the third, no less formidable, feature of a DoS attack is the relative simplicity of its implementation. With the use of off-the-shelf software, a distributed attack can be organized by a group of individuals who have a very poor understanding of the internal organization of computing systems and act only out of hooligan motives.

For ease of analysis, vulnerabilities are divided into classes and subgroups. Information security vulnerabilities can be:

1. objective
2. subjective
3. random.

The methods of implementation can be divided into groups according to the methods of implementation.

- Analytical;
- Technical;
- Software;
- Software and hardware;
- Organizational;
- Social.

Classification of opportunities for the implementation of threats (attacks), is a set of possible options for the threat source by certain implementation methods using vulnerabilities that lead to the implementation of the attack goals. The goal of an attack may not coincide with the goal of implementing threats and may be aimed at obtaining an intermediate result necessary to achieve further implementation of the threat. In the event of such a discrepancy, the attack is considered as a stage of preparation for the commission of actions aimed at realizing the threat, that is, as “preparation for committing” an unlawful action. The result of an attack is consequences that are the realization of the threat and / or contribute to such realization [10].

Information risks are the risk of loss or damage as a result of the use of information technology by a company. In other words, IT risks are associated with the creation, transmission, storage and use of information using electronic media and other means of communication.

IT risks can be divided into two categories:

- risks caused by information leakage and its use by attackers (hackers, competitors or employees) for purposes that could harm the business;
- risks of technical failures of equipment and disruption of the operation of technical means, software installed on them and information transmission channels, which can lead to losses.

The work to minimize IT risks is to prevent unauthorized access to data, as well as accidents and equipment failures. The process of minimizing IT risks should be considered comprehensively:

- Identifying risks;
- Analyzing and assessing the priority of risks;
- Planning responses;
- Minimizing risks. potential problems are identified, and then it is determined in what ways they can be solved.

In practice, ways to identify IT risks do not differ from the methods for determining any other risks: risk maps are drawn up, expert opinions are collected, etc.

To identify the most critical information risks, it is necessary to check the following key points in the security system of an automated system: one. Availability of access control to information systems in which closed information is generated and stored [11]

2.The ability of the system to process external and internal requests and the availability of access to information (authorized) at any time.

3. The ability to integrate existing technologies for working with information in the system for new components in the course of modernization or replacement of the system.

4. Availability of means and methods for protecting information processed in an automated system.

5. The presence of a clear algorithm for actions in a critical situation (failure of computer networks, virus attacks, unauthorized access).

6. Correspondence of the method of processing information resources in the system to the general tasks presented to the automated system.

It is rather difficult to accurately determine the possible damage from most IT risks, but it is quite possible to estimate them approximately.

ЛИТЕРАТУРА

1. Львович Я. Е. Разработка системы автоматизированного проектирования беспроводных систем связи / Я.Е. Львович, И. Я. Львович, А. П. Преображенский, С. О. Головинов // Телекоммуникации. – 2010. – № 11. – С. 2-6.

2. Преображенский Ю. П. Проблемы кодирования информации в каналах связи / Ю. П. Преображенский // Современные инновации в науке и технике. Сборник научных трудов 8-й Всероссийской научно-технической конференции с международным участием. Ответственный редактор А. А. Горохов. – 2018. – С. 180-182.

3. Печенкин В. В. Моделирование динамики серверной нагрузки стохастическими сетями петри с приоритетами (на примере системы видеоконференцсвязи) / В. В. Печенкин, А. Т. Х. Аль-Хазраджи, С. С. Гельбух // Моделирование, оптимизация и информационные технологии. – 2021. – Т. 9. – № 1 (32). –С. 10-11.

4. Преображенский Ю. П. Некоторые проблемы автоматизации процессов / Ю. П. Преображенский // Техника и технологии: пути инновационного развития. сборник научных трудов 8-й Международной научно-практической конференции. Юго-Западный государственный университет. – 2019. – С. 62-64.

5. Клюев С. Г. Проблемы обучения глубоких нейронных сетей для обнаружения угроз нарушения безопасности в сетях с динамической топологией / С. Г. Клюев, Е. Е. Трунов // Моделирование, оптимизация и информационные технологии. – 2021. – Т. 9. – № 1 (32). – С. 15-16.

6. Преображенский А. П. САПР современных радиоэлектронных устройств и систем / А. П. Преображенский, Р. П. Юров // Вестник Воронежского государственного технического университета. – 2006. – Т. 2. – № 3. – С. 35-37.

7. Сычугов А. А. Применение генеративных состязательных сетей в системах обнаружения аномалий / А. А. Сычугов, М. М. Греков // Моделирование, оптимизация и информационные технологии. – 2021. – Т. 9. – № 1 (32). – С. 16-17.

8. Казаков Е. Н. Разработка и программная реализации алгоритма оценки уровня сигнала в сети wi-fi / Е. Н. Казаков // Моделирование, оптимизация и информационные технологии. – 2016. – № 1 (12). – С. 13.

9. Шевский В. С. Разработка алгоритма индексирования данных на основе структуры данных cw-tree с применением параллельных вычислений / В. С. Шевский // Моделирование, оптимизация и информационные технологии. – 2021. – Т. 9. – № 1 (32). – С. 22-23.

10. Львович Я. Е. Исследование методов оптимизации при проектировании систем радиосвязи / Я. Е. Львович, И. Я. Львович, А. П. Преображенский, С. О. Головинов // Теория и техника радиосвязи. – 2011. – № 1. – С. 5-9.

11. Шевский В. С. Технология выполнения поисковых запросов к базе данных на основе метода индексации данных cw-tree / В. С. Шевский, Ю. А. Шичкина // Моделирование, оптимизация и информационные технологии. – 2021. – Т. 9. – № 1 (32). – С. 24-25.

SOME FEATURES OF ATTACKS IN COMPUTER NETWORKS

© 2022 Yu. P. Preobrazhenskiy, E. Zhukov, E. G. Zavgorodniy

Voronezh Institute of High Technologies (Voronezh, Russia)

The paper discusses some features of attacks in computer networks. Examples of possible vulnerabilities are shown.

Keywords: computer network, attack, information protection, vulnerability.