

NETWORK ADMINISTRATION AND SECURITY

Sayfullaev Shakhzod Oybek Ugli

Abstract. *This article provides ideas and considerations about networking and its management and security.*

Key words. *Internet, network, technology, organization, computer, workstation, company, server.*

The creation of Internet technologies has increased the possibilities of obtaining information from various sources quickly and easily for everyone - from ordinary citizens to large organizations. State institutions, scientific and educational institutions, commercial enterprises and individuals began to create and store information in electronic form.


Organizations today rely heavily on computer networks for effective and productive communication. If we assume that each employee has a special workstation, in large companies their number can reach several thousand, and there can also be many servers in the network.

These workstations may not be centrally managed and their environment may not be secure. There are many situations where users exchange messages with different levels of confidentiality, and may have different operating systems, peripherals, software, and protocols. Now imagine that thousands of these workstations on a company network are directly connected to the Internet. This dangerous network containing valuable data with many vulnerabilities makes it an easy target for several hackers to attack.

With the development of computer and communication technologies, the need of all organizations, large or small, to use these high-speed technologies is increasing. Thus, when setting up a network from scratch or upgrading existing network structures, network management and maintenance services from computer maintenance companies are essential. Thanks to these services, the most suitable solutions with high performance but low cost indicators are obtained.

The network technologies and dimensions used by organizations of different sizes are proportional to the scale and size of these organizations. Local area networks (LANs) consist of relatively small systems and communication devices. A wide area network (WAN) is a structure connecting local networks in our country or in different countries of the world.





Network connections are established in different ways. The DSL connection method uses existing telephone lines and provides high-speed data transfer. DSL is a broadband connection technology. ISDN is an international communication standard. It is programmed to send data, images and audio over normal telephone lines. Ethernet technology is also a method of connecting to a network. Computer service companies provide services for these three technologies as per the needs of the organizations.

Within network security, there are three main areas that should be the foundation of any network security strategy: protect, detect and respond. Includes any security measures or policies designed to prevent network security breaches. Diagnostics provides resources to analyze traffic and quickly identify problems before they cause damage. Responsiveness - the ability to respond to identified network security threats and resolve them as quickly as possible. Unfortunately, most businesses don't know how to follow a policy and do it properly. A survey of 4,100 executives, department heads, IT managers and other key professionals across the US and Europe found that nearly three in four organizations (73 percent) are developing a new level of cybersecurity strategy. This is a growing threat because when network breaches occur and malicious threats emerge, more than just the data itself is at risk.

The possibilities of effective use of information led to a rapid increase in the amount of information. Businesses today consider information to be their most valuable asset in many commercial areas. This is definitely a very positive development when it comes to public information and public information. But Internet technologies for secret information flows have created new problems as well as conveniences.

- Remote computer access - programs that allow anonymous access to the Internet or intranet. Logging in to the computer you're running on: based on anonymous computer access programs.

- Disabling the computer remotely - on the basis of programs that connect to the computer remotely through the Internet and stop the operation of it or some of its programs (it is enough to restart the computer to start it).

- Disabling the computer that it is working on - with the help of deactivation programs.

- Network scanners - in order to determine which of the computers and programs running on the network are vulnerable to attack, the network is actually using information gathering programs.




- Vulnerability detection - by searching for vulnerabilities in large groups of computers on the Internet.
- Password cracking - with the help of programs that search for passwords that are easily found in password files.
- Network analysts (sniffers) - using programs that listen to network traffic. They have the ability to automatically extract users' names, passwords, and credit card numbers from traffic.

Protecting the network from computer intrusions is a constant and unsolvable problem. But most network intrusions can be prevented with a few simple security measures. For example, a well-configured firewall and anti-virus software installed on each workstation will thwart most computer attacks. Below is a practical recommendation for securing your Intranet. The security policy should be clear and concise. There should be rules and practices that ensure the safety of the intranet network with clear and consistent steps. A network security system is only as strong as its most vulnerable area. If there are multiple networks within an organization with different security policies, one network may lose reputation due to poor security of another network. Organizations should adopt security policies that ensure the same level of protection is achieved everywhere. The most important aspect of the policy is the development of a single requirement for traffic passing through firewalls. Also, the policy should specify which security tools (for example, intrusion detection tools or vulnerability scanners) should be used on the network and how they should be used, and standard secure configurations should be defined for different types of computers to achieve a uniform level of security. Brandmauer (Firewalls in English) should be used. This is the most basic protection of the organization. Controls incoming and outgoing network traffic (information flow). It can block or monitor certain types of traffic. A well-configured firewall can repel most computer attacks. firewalls, smart cards and other technical and software protection tools should be used wisely.

REFERENCES.

1. Kizza, Joseph Migga. A guide to computer network security. Berlin: Springer, 2017. Print
2. Harrington, Jean L. Network Security: A Practical Approach. Cambridge: Academic Press, 2005. Print o
3. Маллабоев Н., Шокиров Д. СИСТЕМЫ ЭЛЕКТРОННОГО ПЛАТЕЖА //Теория и практика современной науки. – 2016. – №. 6-1. – С. 830-834.





4. Abdullaeva N., Mamurova F., Mallaboev N. EFFICIENCY OF EXPERIMENTAL PREPARATION USE MULTIMEDIA TO ENLARGE SOME QUESTIONS //Экономика и социум. – 2020. – №. 6. – С. 11-13.

