INFORMATION SECURITY ISSUES

N.M.Mallaboyev
Namangan Engineering Construction Institute
Republic of Uzbekistan, Namanagan city, 12 Islam Karimov street

Qozaqova Munojat Sharifjanovna
Namangan Engineering Construction Institute
Republic of Uzbekistan, Namanagan city, 12 Islam Karimov street

Qosimov Muxammadjon
Student, Namangan Engineering Construction Institute
Republic of Uzbekistan, Namanagan city, 12 Islam Karimov street

Chimberdiyev Shukurullo
Student, Namangan Engineering Construction Institute
Republic of Uzbekistan, Namanagan city, 12 Islam Karimov street

The advent of Internet technology has increased the ability to access information from a variety of sources quickly and easily to an unprecedented extent for everyone - from ordinary citizens to large organizations. Government agencies, science and education institutions, commercial enterprises and individuals have begun to create and store information in electronic form. This environment offers great convenience compared to previous physical storage: storage is very compact, transmission takes place instantly, and the possibilities of accessing rich databases over the network are very wide. Opportunities for efficient use of information have led to a rapid increase in the amount of information. Business in a number of commercial areas today considers information to be its most valuable asset. This is definitely a very positive development when it comes to the media and information that everyone can know. But Internet technologies have created new challenges for convenience and confidential information flows, as well as convenience. The threat to information security in the Internet environment has increased dramatically. According to a 1999 survey by the U.S. Institute of Computer Security and the FBI on computer crime, 57 percent of organizations surveyed said their Internet connection was "a place where most attacks occur," and 30 percent said it was. and 26 percent reported that secret information was stolen during the attack. According to the U.S. Federal Center for Computer Crime - FedCIRC, in 1998, nearly 130,000 government networks with 1,100,000 computers were compromised. "Computer hacking" refers to the launch of a special program by people to gain unauthorized access to a computer. Forms of organizing such aggression are different. They are divided into the following types

Remote access to a computer: Programs that allow you to access the Internet or intranet anonymously. Access to the computer on which it operates: based on access programs to the computer without identification. Disabling the computer remotely: Based on programs that connect to the computer remotely via the Internet (or network) and stop it or some of its programs (it is enough to restart the computer to start). Disabling the computer on which it is running: through disabling software. Network Scanners: In order to determine which of the computers and programs running on the network are vulnerable to intrusion, the network is actually through data-gathering software. Finding vulnerabilities in software: Through programs that search for vulnerabilities among large groups of computers on the Internet. Unlock password: by means of programs that search for passwords that can be easily found in

password files. Network Analyzers (Sniffers): Through software that listens to network traffic. They have the ability to automatically separate user names, passwords, credit card numbers from traffic.
The most common aggression has the following statistics:
An analysis of 237 computer attacks conducted by NIST in 1998 was published on the Internet:
29% of attacks occurred in the Windows environment.
Lesson: Unix alone is not dangerous.
In 20% of the attacks, the attackers reached the network elements (routers, switches, hosts, printers brandmauer) remotely.
Lesson: Hosts can be accessed remotely without notice.
5% of attacks were successful against routers and firewalls.
Lesson: Internet network infrastructure developers do not have enough resistance to computer attacks.
4% of attacks are organized to find free hosts that can withstand Internet aggression.
Lesson: It is good that system administrators themselves regularly scan their hosts. 3% of attacks are organized by websites against their users.
Lesson It is not safe to search for information on the WWW.
1999 on the Internet. the most common computer attacks in March. Sendmail (oldest program), ICQ (complex "I'm looking for you" program, used by about 26 million people), Smurf (program that works with ping-packages), Teardrop (error-sensitive program), IMAP (mail program), Back Orifice (trojan horse, for remote control of Windows 95/98), Netbus (similar to Back Orifice), WinNuke (can completely stop Windows 95) and Nmap (scanning program). With the help of WinNuke, Papa Smurf and Teardrop programs, malicious people can attack and damage your computer.
3. Directions of information security
The international standard NIST 7498-2 defines basic security services. Its task is to determine the security aspects of the open system communication model. These are:
Authentication. Authentication of a computer or network user;
Access control.
Check and ensure that the user has access to the computer network;
Data integrity. Checking the contents of the database for accidental or unauthorized changes;
Confidentiality of information. Protecting Content from Unauthorized Disclosure
Inviolability (Neoproverjimost). To prevent the sender from acknowledging that the data set was sent by the sender or received by the recipient. Many additional services (audit, access) and support services (key management, security, network management) serve to complement this basic security system. The complete security system of the web node must cover all of the above security areas. Appropriate security tools (mechanisms) should be included in the software product.
Improving authentication involves addressing the shortcomings of reusable passwords, ranging from disposable passwords to high-tech biometric authentication systems. Items that users carry with them, such as special cards, special tokens or floppy disks, are much cheaper and safer. The unique, module code protected application module is also handy for this purpose. Public key infrastructure is also an integral part of Web node security. The distribution system (people, computers), Public Key Infrastructure (certificate publisher), which is used to ensure authentication, data integrity and confidentiality of information, publishes an electronic certificate. It contains the user ID, its public key, some additional information for the security system, and the digital signature of the certificate publisher. Ideally, this system will create a chain of certificates for the user at any two points on Earth.

This chain allows someone to sign a secret letter, transfer money to an account or enter into an electronic contract, for someone else - to check the source of the document and the identity of the signatory. NIST is working with several other organizations in this direction. Networks have set up firewalls, even though Internet networks have blocked open communication due to hacker attacks.

Without perfect software like PGP, there would be no open network.

Protecting a network from computer intrusions is a constant and intractable problem. But with a series of simple protections, most intrusions into the network can be prevented. For example, a well-configured firewall and antivirus software installed on each workstation (computer) will prevent most computer attacks. The following are 14 practical tips for protecting your intranet. Security policy should be clear and concise. There should be rules and procedures in place to ensure that the intranet security is set in a clear and consistent manner. The more secure a network security system is, the stronger it is. If there are several networks within an organization with different security policies, one network may lose its reputation due to the poor security of another network. Organizations should adopt a security policy so that the expected level of protection is the same everywhere. The most important aspect of the policy is the development of a single requirement for traffic through firewalls. The policy should also specify which security devices (e.g., intrusion detection tools or vulnerability scanners) in the network and how they should be used, and define standard security configurations for different types of computers to achieve a single level of security. Brandmauer (firewalls, English-firewalls,) should be used. This is the organization's most basic means of protection. Controls the incoming and outgoing traffic (information flow) from the network. It can block or control any type of traffic. A well-configured bradmauer can repel most computer attacks. firewalls, smart cards and other hardware and software protection tools should be used wisely.

Brandmauer and WWW-servers should be tested for their resistance to threats of shutdown. Attacks aimed at shutting down a computer are common on the Internet. Attackers are constantly shutting down WWW sites, overloading computers with redundant tasks, or filling networks with meaningless packages. This type of aggression can be very serious, especially if the attacker is smart enough to organize ongoing attacks. Because the source of this cannot be found. Networks concerned about security may organize attacks on themselves to estimate the damage that would result from such attacks. It is advisable to conduct such analyzes only by experienced system administrators or specialized consultants. Cryptosystems should be widely used. Attackers often infiltrate the network by listening to traffic passing through its important locations, using users to separate the traffic and their passwords. Therefore, connections to remote machines must be encrypted when they are password protected. This is especially necessary when the connection is made via Internet channels or connected to an important server. There are commercial and free programs for encrypting TCP / IP (the most popular SSH) traffic. Using them will prevent aggression. The most reliable means of protecting the flow of information and resources on the Intranet, combined with the Internet environment, is the joint use of symmetric and symmetric cryptosystems. Computers need to be configured competently from a security standpoint. When operating systems are reinstalled on a computer, they are often vulnerable to intrusion. This allows the attacker to use many methods to attack the car. Therefore, all unnecessary network tools should be disconnected from the computer. Patching. Companies are constantly making corrections to fix bugs found in their programs. If these errors are not corrected, the attacker can use it to attack your program and through it your computer. System administrators must first protect the necessary hosts by installing fixes to programs on their most essential systems. This is because fixes occur frequently and you may not have time to install them on all computers.

Generally, adjustments should only be made by the company that developed the software. Be sure to correct any deficiencies encountered in intranet security. They should also use the other protective equipment listed below. Intrusion Detection should be used. Aggression detection systems detect aggression by operational detection. To detect intrusions from within the network, they are placed behind the firewall, and in front of it to detect intrusions to the branmauer. Such tools have different capabilities. More information can be found at the following site. http://www.icsa.net/services/consortia/intrusion/educational_material.shtml You should try to detect viruses and "Trojan horse" programs in a timely manner. Antivirus software is an integral part of protection for the security of any network. They monitor the computer and find malware. The only problem they cause is that they must be installed on all computers on the network and regularly updated to ensure maximum protection. It takes a long time to do this, but otherwise the engine will not give the expected effect. Computer users need to be taught how to do this, but only if they are not given the task completely. In addition to anti-virus software, you also need to scan applications for emails on the mail server. In this way, the path of viruses that can reach users' computers is blocked. The tolerant spaces should be scanned. Such scanning software scans the network to find computers that are vulnerable to certain types of intrusions. They have a large database of vulnerabilities, which can be used to find out if there is a vulnerability on one computer or another. Commercial and free scanners are available. System administrators should periodically find such computers for their programs in a timely manner and take appropriate action. The risk level should be assessed to identify vulnerabilities in the protection of individual devices. It is necessary to determine the network topology and enable port scanners. Such programs provide a complete picture of how the network is structured, what computers work on it, what services are performed on each machine. Attackers use these programs to detect malicious computers and programs. Network administrators also use such software to determine which programs are running on which computers on their networks. This is a good tool for finding incorrectly configured computers and making corrections to them. You must use Password Crackers. Hackers often try to use computers to steal encrypted files with passwords. They then run special programs that decrypt and use them to find the passwords in these encrypted files. Once such a password is obtained, they use different methods of accessing the computer without notifying the computer and the network, just like a normal user. Although this tool is used by malicious people, it is also useful for the system administrator. System administrators should periodically find such passwords to their encrypted files in a timely manner and find appropriate passwords to take appropriate action. You need to be vigilant with regard to war dials. Users are often allowed to receive incoming phone calls to their computers by bypassing the organization’s network protection tools. Sometimes, before returning from work, they connect the modem to the computer from home, connect it to the modem and use the network to set up their programs. Attackers try to call many phone numbers using combat communication software, thus infiltrating such networks, allowing access from the outside via a modem. Because users often configure their computers themselves, such computers are poorly protected from intrusions, creating another opportunity for network intrusion. System administrators should regularly use combat communication installers to check their users' phone numbers and take timely action to find computers configured accordingly. There are commercial and free distributed combat communication software. You should be aware of security advisories in a timely manner and follow them. Security Recommendations - Warnings issued by computer crime teams and software developers about software vulnerabilities that have recently been identified. The recommendations are very helpful, take very little time to read, and warn of the most serious risks that can occur due to overlooked hazardous areas. They express the risk and give tips to

prevent it. They can be obtained from a number of places. The two most useful recommendations are the ones published by the Computer Crime Team and can be found on the CIAC and CERT sites. A safety incident investigation team should be involved on a regular basis. Security-related incidents can occur in any network (even if it is a false alarm). Employees of the organization must know in advance what to do in this or that case. When to contact law enforcement, when to call a computer crime team, and when to disconnect the network from the Internet, and what to do when an important server is broken. CERT provides advice in this regard within the United States. FedCIRC is responsible for providing advice to U.S. public and government organizations. It is advisable to have such counseling centers in every state.

References:

1. Sharifjanovna, Q. M. (2021). Perpendicularity of a Straight Line to a Plane and a Plane to a Plane. International Journal of Innovative Analyses and Emerging Technology, 1(5), 70-71.
2. Abduraximovich, U. M., & Sharifjanovna, Q. M. (2021). Methods of Using Graphic Programs in the Lessons of Descriptive Geometry. International Journal of Discoveries and Innovations in Applied Sciences, 1(6), 149-152.
3. Комилов, С., & Козокова, М. (2015). Разработка вычислительного алгоритма решения гидродинамических задач управления процессами ПВ в неоднородных средах при условии использования этажной системы разработки. Молодой ученый, (11), 324-328.

.