Cyber Security Measures In Companies

Mladen Vukašinović

Abstract—**Proposal of cyber security measures in companie. Cyber security is currently the most wanted and most challenging research discipline that is in constant development. Data reference institutions and recognized to security researchers in 2017 shows that cyber criminals using 'low-tech' 'software were successful in 9 of 10 attacks on various web sites. Most web sites had serious flaws for a period of 150 days or more. Various invasions and fraud have cost the company $ 6.6 billion annually. Based on the research of Oracle java in America is the biggest security risk for desktop computers. According to reports java is installed on 65% of computers, 48% of users did not have the latest patches for Java last year been identified 119 new vulnerabilities in the software. According to research, mobile phone users are increasingly exposed to cyber attacks. Based on analysis of more than 400 000 applications available in the most popular apps and Google applications 14 000, or 3% have security vulnerabilities, including sensitive information such as location, text messages and contacts. In this work will be given to the proposal of measures that could improve the protection of computer systems from unauthorized intrusion.**

Keywords—Cyber security; Security vulnerabilities; Protection of computer systems;

I. INTRODUCTION

It is estimated that the Internet uses about 3.3 billion inhabitants [4] and that about 9.9 billion computers, mobile phones and other devices around the world are connected to the Internet. This number is constantly increasing, which also contributes to the fulfillment of increasing security requirements. The most common security problem on the Internet is viruses that occur on a daily basis. The easiest way for cyber criminals to fall into the computer system is through them. It is necessary to choose the appropriate operating system that is stable, reliable and resistant to most destructive programs. It is also necessary to install appropriate antivirus programs that can, before acting, detect and destroy or disable such programs. Good protection is taking maximum precautions when downloading files from the Internet and opening an email account, creating backups of all relevant data, updating the program (downloading and installing stoves) [1], etc A large number of security threats to the system of large networks are already committed attacks that have not been detected. According to Verizon's research, as much as 66% of the decline remains undiscovered for months and the viruses remain undetected in the system and over 200 days in those companies [2]. So special attention should be paid to the protection of undisclosed attacks and viruses. It is necessary to use monitoring systems and early detection algorithms, notification and possible automatic response to system failures

The paper will outline the basic measures that should be implemented to raise the level of security and security of cyber attacks.

Mladen Vukašinović University of Montenegro UCG
Podgorica , Monte Negro
e-mail: bigmazy@hotmail.com

II. PROTECTION OF COMPUTER SYSTEM FROM CYBER ATTACKS

Cyber security attacks are divided into two groups of attacks: passive and active attacks. In passive attacks, an attacker gets rights without changing the content of messages (an attacker listens and analyzes traffic between two workstations). In active attacks, the attacker can change, delete, copy the contents of files, identify him as an authorized user, disable normal data flow, etc.

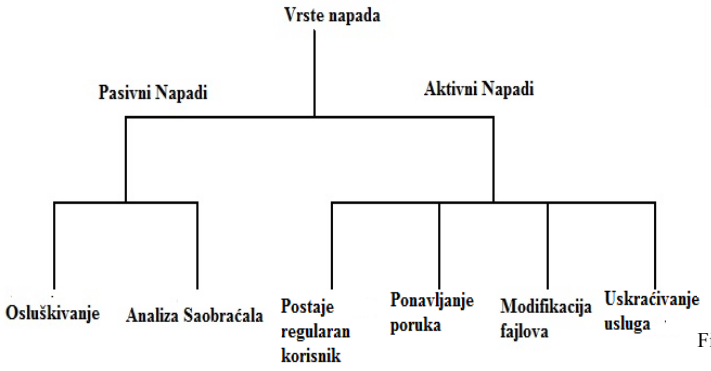

Fig 1. Network attack segments

The protection of network systems should be ensured through three conditions: confidentiality (confidentiality, to prevent intentional or unintentional unauthorized decline), integrity (integrity-ensuring the accuracy and integrity of information) and availability (availability-reliable access to data and resources) of data and resources . It is necessary to provide a high-quality firewall and monitoring system. Then Intrusion Detection System and high-quality advanced antivirus scanners. This involves building a layered defense from crashing into the system, detecting an infection in a timely manner, and using the defense once you have been infected. To do this, you must go beyond the security range and implement an advanced protection process that includes: Advanced detection: traffic analysis and use of knowledge forms that know when an attack is formed. Total retention: when an attack is detected, ensure that the attack stops [2]. Hazard Identification: Use as a key learning tool that will improve your defense over time. Advanced mitigation of the threat: this should include removal of infection, recovery of the disadvantaged system, and all recovery efforts after that.

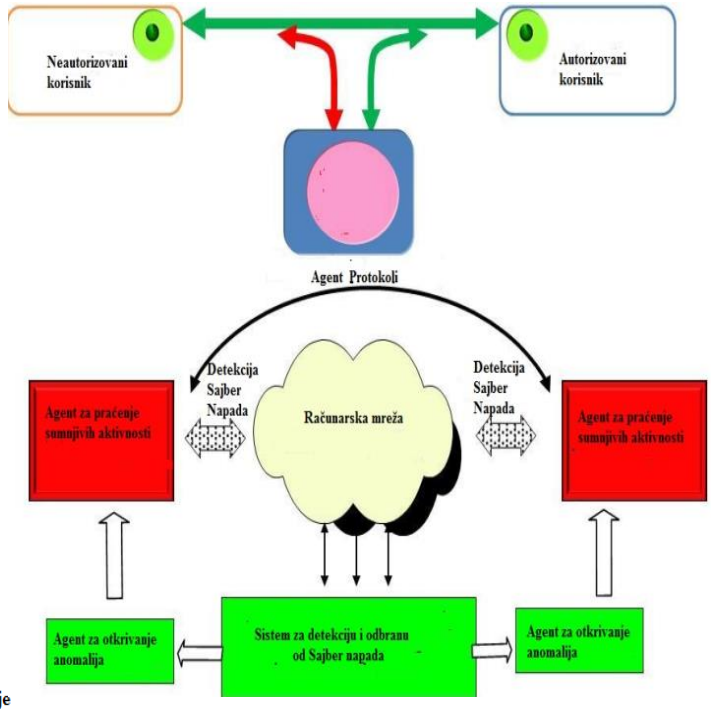

Fig 2. Scheme of the Cyber Detection System

Special attention should be paid to the protection of server machines.

First, it is necessary physically to provide the system with a server room (installing cameras with motion sensors, entering the authorized person's room with an identification card, fingerprint, etc.). A few people should have the same right to control the entire network. There should be a controller of all persons who have authorized access.

Then a demilitarized zone is needed (dmz-demilitarized zone-part of the network that does not belong to the local network or is part of the external network). All protected servers must be located in this protected zone (e-mail server, server database, dns server, ldap, proxy server, web server, etc.). In this case, there is a protective barrier layer between the local network and public servers, which increases the safety of the internal part of the network. DMZ can be created by placing triple protective walls. These are firewalls that make a triple interface, one is to the local network, the other to dmz, and the third is to the Internet.

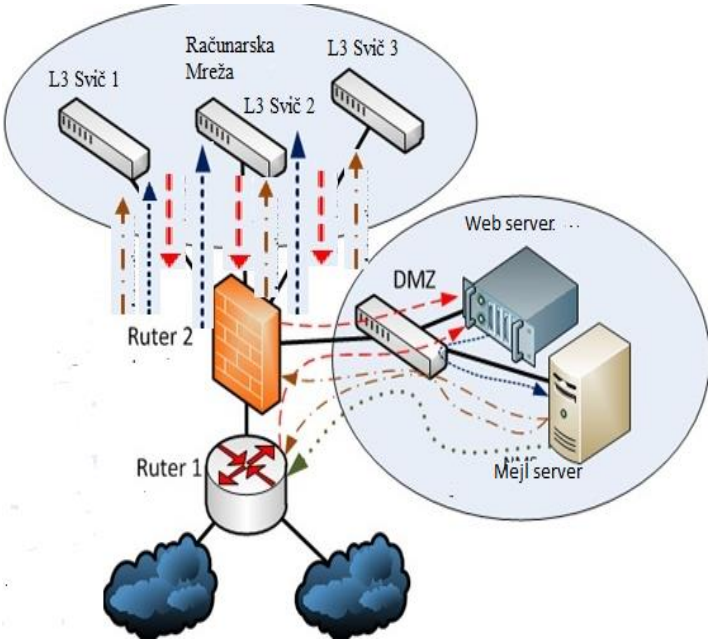

Fig 3. Schematic of the Triple Protective Wall

System security is significantly enhanced by using encryption systems (for example, https based on ssl / tls protocol), virtual private networks and antivirus scanners.
IT administrators on all servers should block the possibility of remote logging. The only option for working on servers should be directly on the machine itself. It is necessary to create strong administrative passwords on servers. Use a combination of at least 23 characters combined with small, capital letters, numbers, and special characters (#,!,%, Etc.). All passwords need to be changed a month.
Since the email service is one of the most used services and via e-mails, a large number of viruses are easily sent, it is necessary to additionally protect the mail server. This can be done by setting up a network gateway (IMP). IMP includes a number of security features, such as virus scanning functions, removal of email related files, filtering message content, blocking spam messages, and preventing attacks. For confidential sending of data electronically, it is necessary to create an internal email server that can only send e-mails internally, without the possibility of sending and receiving e-mails, as well as from the Internet.
Regarding the protection of the computer network from the users themselves, IT Administrators during the working hours should prevent users from using internet content that poses security threats to the computer system (social networking sites, adult content sites, online games, etc.). All users must have user and not administrative tasks on their computers, and all must have access passwords. Security systems need to be designed and implemented (openBSD, Linux, Mac OS X, etc. [5]), security rules, encryption, authentication.
All operating systems should have the latest security patches (stoves) installed, and all antivirus software on computers must be updated on a daily basis. Multiple backups of data backups should be made on a daily basis and stored in several different locations, outside the premises of the company in well-protected areas.

Deep protection

One lesson in computer science is that security solutions do not create peace.
IT security recognizes the concept of "deep security", and multiple security layers are in the network environment. This method protects against attacks by using many independent methods. A more detailed approach to defense is intended to prevent and / or prevent conflicts and to detect or respond to theft, thereby reducing potential impacts.
Each ICS environment is different. There is no solution for everyone. The traditional security features are designed to detect, ban, or delete cyber risks. However, computer criminals are more capable and can not detect and stop the virus before entering the network.
More cyber-attacks include things that seem intentional for long periods of time to avoid suspicion. Monitor monitoring and intelligent protection against such progressive attacks, capable of recognizing this behavior.
To improve the efficiency of products related to safety, many organizations implement different layers of solutions in different configurations. For example, the four types of security solutions that make up the backs of any defense strategy on the right are:
External clouds, internet browsers,
Data diode;
firewall; and
Network segmentation devices.
These systems need to be subject to regular monitoring of information so that they meet the security needs of the enterprise.

Increase network access

Most malware attacks and computer attacks are caused by Internet access, so you may find it easier to secure the network's network if you do not need an internet connection. However, some security admins want to offer full access to the network.
In order to solve this problem, a new form of Internet Gateway has been successfully scanned by the external cloud. This solution can secure a secure external website connection. This solution can be fully protected from infiltration, harmful operation and control.
Internet access can not penetrate corporate networks when outside the network threats. Network users may be able to run and install disk drives and other applications, but the attack is limited to cloud based web applications received when the net returned the virtual machine. The malicious software installed on the corporate network - e-mail, USB memory, and other devices can not easily connect with drivers on the internet.

Data diode and firewall

Data diodes are a simple segmentation device and are a very effective security tool that is used in high security environment. For one side gateway, information is only transmitted in one direction. Because the data diodes are hardware solutions, their integrated solutions can not be destroyed by online software attacks and virus-dependent infiltration.

The key advantage of the Diode is that it provides a great deal of resources to store the confidentiality of landing platforms that are more important in the OT environment. The Diode also protects the original data and integrity of the system against object attacks. It is best to remotely control the system without unloading the remote system.

It is interesting to use diodes because it is easy and cost-effective compared to other solutions, but it is very important to check whether the data in a directional flow is really appropriate. For example, when segmentation and access control is required, segmentation devices may be a better solution.

Firewalls enforce network packet rules based on network packets or more advanced metadata data and check against packet badges that define content for each packet. It can be effectively prevented from visible or known network attacks.

Some years ago, there were only a few viruses and malicious programs in the IP environment. Currently, ICS networks play an important role in cyber criminals and other sophisticated groups. The latest ICS gateway supports a variety of protocols and adds policies and rules based on the content of all protocols and protocol versions.

A new generation of firewalls allows for advanced search

III. Conclusion

For now, there is no fully protected computer network. The most secure system is one that is not connected to the Internet connection, which has its original internal operating system on computers and has a high level of security protection.

The protection of network systems should be provided to enable the prevention of intentional or unintentional unauthorized intrusion into the system both from the outside and from the inside, ensuring the accuracy and integrity of information and reliable access to data and resources.

Early indetermination and monitoring systems need to be used to reduce the security risks of intrusion into systems.

The paper presents measures that if fully implemented, would maximally protect the company's computer systems.

References

[1] Peter Szor, The Art of Computer Virus Research and Defense, Addison-Wesley, 2005 – Computers

[2] Ubm tech Cybersecurity – You're Already Compromised, feb., 2015.

[3] By CSO, article, By the numbers 2015: The year in security research, dec., 2015.

[4] http://www.internetlivestats.com/internet-users.

[5] https://www.secpoint.com/top-10-most-secure-operating-systems.html.