DOI 10.26411/83-1734-2015-1-45-4-20

Network Security - Security Methods in Transnational Corporations (TNC)

Katarzyna Witczyńska
University of Wrocław, Poland

Modern times are associated with a huge increase in the number of security breaches in transnational corporations. The conclusion is that all preventive measures should be taken to stop the growing online crime in globalizing economies. Nowadays, when the Internet is becoming more and more common and more people use its resources, security becomes a priority. The use of firewalls, IDS and IPS systems, the implementation of appropriate security rules, the awareness of network users and the continuous deepening of knowledge in this area can significantly contribute to the security of data of transnational corporations.

Keywords: Network security - programs, tools and applications, Pretty Good Privacy

1. INTRODUCTION

Nowadays, the number of security breaches in the transnational corporations is increasing dramatically. It follows that all preventive measures should be taken to stop developing cybercrimes in globalizing economies. The Internet is becoming more and more common and more and more people are using its resources and thus security becomes the highest priority. The use of firewalls, IDS and IPS systems, the implementation of appropriate security policies, the awareness of network users and the continuous improvement of knowledge in this area can significantly contribute to the increased security of transnational corporations.

2. NETWORK SECURITY - PROGRAMS, TOOLS AND APPLICATIONS

Security policy should be a centre of increased attention in order to secure, monitor, test and improve the TNCs network. Security procedures that determine the configuration, logon, audit, and host and network management processes are used to implement this policy. In addition, you can minimize the risk by establishing clear rules how to deal with security breaches. These procedures may include simple activities - such as managing and updating software. On the other hand, they should contain complex implementations of firewalls and intrusion detection systems. Examples of tools and applications used to secure your network:

- Firewall - a hardware or software security tool to detect network traffic.
- Spam blocker - installed software (server or user computer). This is to identify and destroy unwanted messages.
- Patches and updates - software for your system or application to repair security vulnerability or to add useful functionality.

- Spyware protection - software installed on your PC to detects and removes spyware and adware.
- Pop-up blockers - software installed on your computer to avoid the continuous appearance of your ads.
- Virus protection - software installed on your computer to eliminate worms and Trojans.

Security authorization and authentication - providing access to dedicated resources on the Internet to specific users is provided after verification their identity. Authorization is a process that confirms that a user is the person claims to be (after authentication) and has the right to use the resources which is trying to access. For example: users to enter on a web site must have their name and a valid password. After authentication, they are assigned specific permissions. One type of authentication that includes the password is the Personal Identification Number (PIN). The purpose of authentication is to determine whether the cardholder is the legitimate user of PIN. Other methods of authentication are: recognition of the user's fingerprints or hand vein system, retinal scan systems and voice recognition [1].

All websites with SSL have a URL that starts with HTTPS: //. Sites that do not start with this address are not encrypted, so while using these sites one should not provide sensitive data and information such as credit card numbers. Web browsers also have additional SSL secure connection pointers. In web browsers such as Internet Explorer, a padlock appears at the bottom of the window, and a key appears in the Netscape Navigator at the bottom of the window. In case of a visible key or padlock in the browser, the data exchanged between an Internet user and the server is encrypted and secured [2].

PGP (Pretty Good Privacy) is a software encryption system. It is used to protect your e-mail and attachments. Mail programs such as Microsoft Outlook Express, Eudora and Microsoft Outlook can use PGP extension modules. These modules are installed in the e-mail program and appear in the menu options or as buttons in the mail program window. PGP gives you the ability to digitally sign letters, thereby ensuring the authenticity of your email messages. Each document and user has a unique digital signature. In case when one user sends two different documents, they will have other digital signatures, because their shortcuts (on which the checksums are created) will be different [3].

3. FIREWALL

The term "firewall" originally referred to a wall intended to limit a fire or a potential fire in a real building [4]. Next applications refer to similar structures, such as metal sheet separating the engine compartment of a vehicle or a passenger compartment [5].

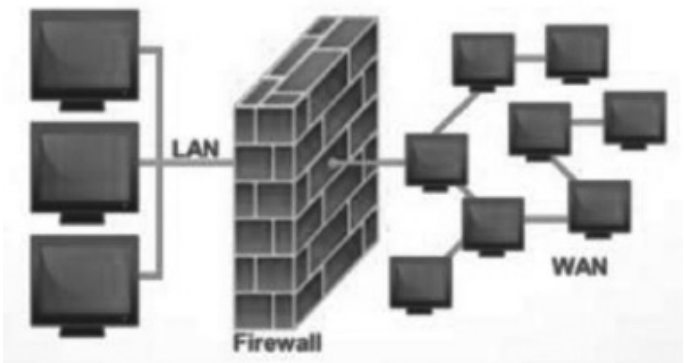

Fig.1. Firewall

In a computer language, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predefined security rules [6]. A firewall usually establishes a barrier between a trusted, secure internal network and an external network, such as the Internet, which is assumed to be unsafe or untrusted. Firewalls are often classified as network firewalls. Firewalls filter traffic between two or more networks; software devices running on general purpose hardware or computer hardware firewalls. Host-based firewalls provide a software layer on a single host that controls network traffic to and from the same machine [8].

Firewalls can be classified in two ways. The first classification divides the firewall into hardware and software.

- Firewalls are specialized devices that are located on the edge of a local area network and are responsible for filtering traffic. Often, they also provide an address mapping (NAT) feature that allows you to create independent local networks. They often have web gateway functions, as well as a router, DNS server, or DHCP server.
- Software firewall - programs (or operating system components) that perform similar functions as their hardware counterparts.

The main difference is that they need a computer with an operating system installed and a configured network connection or network connections. The second division is distinguished by two types of network firewalls: filtering and intermediary.

- Filtered network firewalls - monitor the network packets passing through them and only let pass those that conform to the established rules. Desktop software provides selected ports used to receive incoming connections; monitors traffic; also makes outgoing calls from your computer to selected services / programs. They operate at a low network level (layers 3 and 4 ISO / OSI). They have the ability to filter packets at the IP address level (e.g. by blocking communication with specific addresses) and ports (allowing access to specific services).
- Proxy-based firewalls - make connections on behalf of the user. They work at a high level (ISO / OSI application layer). They analyse the content of the package not because of its origin and destination, but in terms of transferred content. They mediate between the source and the destination. Communication takes place in two stages. The first step is to connect to the firewall server and send information about the required data and the source of their download. In the second stage, the firewall connects to the indicated source and retrieves the data by analysing their contents. Next it sends the received data to the computer waiting for them. Intermediate firewalls can detect and block invalid packets that could be handled by a local system when connected directly.

4. INTRUSION DETECTION SYSTEM (IDS)

The primary purpose of the Intrusion Detection System (IDS) is detection of threats in a computer network. The primary task of intrusion detection is to monitor network traffic. Intrusion detection is based on information about the activity of the protected system. Current IDS systems research real-time network activity. IDS investigate the processes that take place in the main areas of networks that are protected. This action serves to uncover the trials. This is very important for security reasons that after successful hacking IDS works biphasically even if an intruder can break into the system, it can still be discovered and annihilated although it wants to destroy the traces of its activity. IDS systems use four main methods to identify an intruder inside a protected network:

- Matching patterns - the easiest way to detect an intruder; single packet is compared to a list of rules, and immediately after a positive verification, an alarm is triggered.
- Contextual pattern matching – in context matching of the package, the system takes into account the context of each package. So the above system tracks the connections and binds the fragmented packets.

- Heuristic analysis - uses algorithms to check for malfunction. They are usually a statistical evaluation of normal network traffic. For example, the port scan algorithm shows that this is the case if an attempt is made to connect to multiple ports from a single address shortly.
- Analysis of anomalies – signatures of anomalies try to detect abnormal network traffic. The biggest challenge is to determine what is considered normal.

5. SUMMARY

Ensuring complete security of networks and IT systems is not possible. This is related to the inevitable occurrence of computer programming errors and the lack of predictability of the methods used by Internet hackers. The highest level of protection is the enhancement of user awareness, the use of proven packet solutions in the cloud, and decision-making based on common sense.

REFERENCES

[1] Wojciechowski A., *Usługi w sieciach informatycznych*, Mikom, Warszawa 2006.

[2] Bowen R., Coar K, *Apache. Receptury*, Wydawnictwo Helion, Gliwice 2009.

[3] Karbowski M., *Podstawy kryptografii,* Wydawnictwo Helion, Gliwice 2007.

[4] Cortada J. W., *The Digital Hand,* vol. 3: *How Computers Changed the Work of American Public Sector Industries,* Oxford University Press, s. l. 2007.

[5] Canavan J. E., *Fundamentals of Network Security*, Artech House, Boston 2001.

[6] Noureddine B., *Security of mobile communications,* CRC Press, Boston 2010.

[7] *Oppliger R., Internet Security: FIREWALLS and BEYOND, "Communications of the ACM", 40 (1997)/5, pp. 92-102.*

[8] *Vacca J. R., Computer and information security handbook, Elsevier, Amsterdam 2009.*

Katarzyna Witczyńska
University of Wrocław, Poland
k.witczynska@uwr.edu.pl