Network Security: A Shield to the Users
Swastika Aggarwal¹, Swati Sharma²

¹B.TECH Student, ²Research Guide, Northern Institute of Information & Technology.

Abstract

The integration of Internet and mobile Internet, Internet of Things (IOT), promote the wide application of the industrial Internet and other vertical Internet. The Internet is spreading widely with a tremendous speed and with the spread of Internet, the security concerns are also increasing. Traditional networks of a variety of viruses, hackers and other threats expand the network to the new system, they cause damage to the system. In this paper, there is the introduction of network security, types of network security, benefits of network security combined with the safety requirements and the analysis on the level of safety requirements as well as the approaches of security detection.

Keywords: Attacks, Internet, Network security, Threats

Introduction

The network security is any activity that is designed to protect the usability and integrity of our network and data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on our network. It deals with the requirements needed for a company, organization or the network administrator to help in protecting the network.

We are all connected to the Internet without any boundary to make our life comfortable. So, network security is very important to protect the network and even ourselves from the network attacks. Network security is a challenge for network operators and Internet Service Providers (ISPs) in order to prevent it from the attack of intruders. Network security can be referred as protecting website domains from various forms of attack. If we have the knowledge of how various attacks are executed, we can protect ourselves.

Need of Network Security: Network security is the process through which we can protect the digital information. It is so crucial for all networks must be protected from threats and the risks so that a company, organization or business can achieve its fullest potential.

The objective of network security is to protect the confidentiality, to maintain integrity, to ensure availability. We are dependent on computers today for controlling large money transfers between banks, insurance, markets, telecommunication, health and medical fields and so on. So, we cannot negotiate security in these critical areas. Now our need of network security has broken into two needs—one is the need of information security and other is the need of computer security. On the Internet or any network of an organization, thousands of important information is exchanged daily. This information can be misused by the attackers.

So, the information security is needed for protecting the secret information users on the net only. It is needed to protect the information from unwanted editing, accidentally or intentionally by unauthorized users. It is needed to protect the data from wandering the data packets or information packets in the network foe infinitely long time. The computer security is equally important and should be protected from replicating and capturing viruses from infected files. It is also needed to protect the message from unwanted delay in the transmission lines/route in order to deliver it to the required destination in time, in case of urgency.

Types of Network Security

Application Security: Any software we use to run our business needs to be protected, whether our IT staff builds it or whether we buy it. Unfortunately, any application may contain holes or vulnerabilities that attackers can use to

Corresponding Author: Swati Sharma, Research Guide, Northern Institute of Information & Technology
E-mail Id: swatiii.harit@gmail.com
Orcid Id: https://orcid.org/0000-0003-1745-2348
How to cite this article: Aggarwal S, Sharma S. Network Security: A Shield to the Users. Int J Hum Comp Inter Data Min 2018; 1(1&2): 15-17.
infiltrate our network. Application security encompasses the hardware, software and processes we use to close those holes.

**E-mail Security:** E-mail gateways are the number one threat vector for a security breach. Attackers use personal information and social engineering tactics to build sophisticated phishing campaigns to deceive recipients and send them to sites serving up malware. An E-mail security application blocks incoming attacks and controls outbound messages to prevent the loss of sensitive data.

**Firewalls:** Firewalls put up a barrier between our trusted internal network and untrusted outside networks such as the Internet. They use a set of defined rules to allow or block traffic. A firewall can be hardware, software, or both.

**Web Security:** A web security solution controls our staff’s web use, blocks web-based threats and deny access to malicious websites. It protects our web gateway on site or in the cloud.

**Intrusion Prevention Systems:** An Intrusion Prevention System (IPS) scans network traffic to actively block attacks. CISCO Next-Generation IPS (NGIPS) appliances do this by correlating huge amounts of global threat intelligence to not only block malicious activity but also track the progression of suspect files and malware across the network to prevent the spread of outbreaks and reinfection.

**Network Segmentation:** Software design segmentation puts network traffic into different classifications and makes enforcing security policies easier. Ideally, the classifications are based on endpoint identity, not mere IP addresses. We cannot assign access rights based on role, location, and more so that the right level of access is given to the right people and suspicious devices are contained and remediated.

**Behavioral Analytics:** To detect abnormal network behavior, we must know what normal behavior looks like. Behavioral analytics tools automatically discern activities that deviate from the norm. Our security team can then better identify indicators of compromise that pose a potential problem and quickly remediate threats.

**Categories of network security threats:** Network Security threats are becoming increasingly sophisticated and dangerous because Internet is an increasingly attractive hunting ground for hackers, criminals, activists and terrorists motivated to get noticed, make money or even bring down corporations and governments through different threats of attacks.

Network security threats can be categorized into four broad themes:

**Unstructured Threats:** Unstructured threats mostly originate from inexperienced individuals using easily available hacking tools. These types of intruders are not most talented or experienced programmers or machine operators but they are those motivators who have ample of time to do something challenging.

**Structured Threats:** Structured threats are imposed by individual or a group who are highly motivated and are technically strong also. Occasionally, these intruders are hired by industries, some intelligence agencies, etc.

**External Threats:** External threats are originated from individuals or groups working outside of the organizations. They do not have authorized access to any of the computer systems or the network. They contact the organizations network from the Internet or from the dial-up access servers.

**Internal Threats:** Internal threats originate from inside the organizations itself from a dissatisfied current or a former employee.

**Benefits of Network Security:** Network Security has a number of benefits for defending our information or data against threats. It has the benefit of minimizing the level of risk for attacks, infections and breaches.

Network security keeps sensitive data such as personal information and confidential business materials away from unauthorized individuals.

Network Security denies spyware. Spyware is a form of cyber infection which is designed to spy on our computer actions and relay that information back to the cyber-criminal. Great cybersecurity can prevent this spyware from taking effect and ensure that our employees’ actions remain private and confidential within our workplace.

Cyber crime is constantly on the rise and many businesses and organizations are extremely vulnerable as a result of ineffective cyber security. IT security solutions are essential for all kinds of businesses, particularly when we think about how important the Internet and our digital systems are for our day-to-day operations.

**Network Security Challenges:**

- Malware with worm capabilities
- Getting back to basics (patching, endpoint, hygiene)
- The vulnerability of mobile carriers
- Stop overwhelming clients with alerts
- Adapting the firewall to face new threats
- Monitoring cloud configuration and security
- High impact attacks and the insider threat

**Conclusion**

Network Security attempts to ensure the confidentiality, integrity and availability of computing systems and their
components. The security situation arises in our everyday Internet activities and sometimes it is really difficult to distinguish between a security attack and an ordinary human or technological breakdown. Sometimes several controls are needed to cover a single vulnerability, but sometimes one control addresses many problems at once. To determine the necessary security technologies, the security threats and Internet Protocol should be analyzed. An effective network security plan should be developed with the understanding of security issues, potential attackers, needed level of security and factors that make a network vulnerable to attack. Tools to reduce the vulnerability of the computer to the network include encryption, authentication mechanisms, intrusion detection, security management and firewalls. In addition for protecting the network from outside threats, enforcing company network usage policies can prevent internal users from pulling in threats due to misuse.

References

5. What is network security and why we need network security, Omni Secu.com.
7. Types of Network Security, Cisco.

Date of Submission: 2018-03-27
Date of Acceptance: 2018-04-24