Example of networking security threats and countermeasures essay

Sociology, Communication

Networking Security Threats and Countermeasures

In today's " networked" environment, security is a must and a foremost concern for everyone connected to the network. Taking security countermeasures for granted could mean destruction of the person or the company being attacked. Although, joining a network has a lot of benefits including greater and easier access to data, data should never be compromised. Network security must be a priority for everyone connected to a network to " prevent loss, through misuse of data" (Sundaram, 2010) which is its main purpose. Network security does not only mean securing the computers at the end of the communication line. It also includes security along the communication lines.

There are a lot of networking security threats which can be broadly categorize into passive and active security attacks. Passive attacks or security threats includes eavesdropping on the network line while active attacks includes impersonations. These network threats can also be group according to threats that can affect the integrity, confidentiality and authentication. (Stallings, 2011)

Threats that affect the integrity of data can include data modification, Trojan horses, memory modification and message modifications. These can result to loss of information and vulnerability to other attacks as well as obliteration of the machines in use. (Stallings, 2011) Trojan horses are programs that appears to be benevolent but usually carries a virus with it. (Daya, 2009) Cryptographic checksums, a way of testing and verifying files at a later date using complicated series of mathematical operations, are usually used as countermeasures to this attack.

Confidentiality threats usually involves eavesdropping, theft of information both from the server and the client, as well as information on the networks configuration which could result to loss of both privacy and information. (Stallings, 2011) Any form of attempt to obtain confidential data is generally referred to as phishing. Common countermeasures applied to these types of attacks are data encryption and application of firewalls. Firewalls are usually applied to prevent incoming traffic from outside the network from coming in. (Daya, 2010)

Data forgery and impersonisation on the other hand, are common threats that affects authorization. The most common countermeasures applied involves cryptographic measures through the use of codes and ciphers to convert data into unintelligible codes. Other countermeasures being implemented today to prevent these attacks are the usage of Intrusion Detection Systems (IDS) in the form of both hardware and software, the installation of Anti-Malware and Anti-Virus Software for malicious software detection and implementation of a set of protocols called Secured Socket Layer (SSL) which uses certificates as a means of authentication. (Daya, 2010)

References:

Daya, Bhavya (2010). Network Security: History, Importance, and Future. Retrieved from http://web. mit. edu/~bdaya/www/Network%20Security. pdf

Google (2013). A Google’s Approach to IT Security. Retrieved from https://cloud. google. com/files/Google-CommonSecurity-WhitePaper-v1. 4. pdf

Lou, Zhou (2010). Review and Evaluation of Security Threats on the Communication Networks in the Smart Grid. Retrieved from http://apachepine. ece. ncsu. edu/publications/10llww-milcom. pdf

Stallings, William (2011). Cryptography and Network Security: Principles and Practice. Retrieved from http://www. google. com. ph/url? sa= t&rct= j&q=&esrc= s&source= web&cd= 2&cad= rja&ved= 0CDUQFjAB&url= http %3A%2F%2Fwww. cs. iit. edu%2F~cs549%2Flectures%2FCNS-1. pdf&ei= _548UYWABbCaiAf9r4CoCA&usg= AFQjCNFctUEp0nDK0QnU2SU29dVMnngJQw&bvm= bv. 43287494, d. aGc

Sundaram, Karishma (2010). Why is Network Security Important?. Retrieved from http://www. brighthub. com/computing/enterprise-security/articles/69275. aspx