Sebastian Cappadonna

CS320

Sayed Khushal

November 13th of 2020

Prevention of security threats to the networks

Since the beginning of the semester, a lot of security prevention has been discussed regarding which are the most commons, what they are, etc. Thus, some of the most commons threats to the network researched for the presentation were, Viruses, Worms, Adware, Spyware, DDoS attacks, Phishing attacks, Ransomware, Cryptojacking, and APT Threats. Having stated the threats, it is good and important to mention the correct preventions or measurements in order not to have our network affected considerably. Therefore, in the following paragraphs, we will be discussing each of the threats, explaining ways where they can be prevented to infect the networks.

It is essential to mention the definition of a Threat, which is anything that can take advantage in order to breach security and harm an object of interest. Some threats that can be considered are Software attacks, theft of intellectual property, identity theft, and information extortion. Therefore, a Threat to the Network would be defined as anything that can be taken advantage of, and cause considerable damage to the network system, in a way where it can lose important information, damage the whole network, and slow the processes of the network as well.

Firstly, Computer viruses and worms are damaging malicious programs designed to infect network systems, destroying essential systems data, and making the network inoperable. However, Viruses are connected to a system or host file and usually are activated by a timer or by opening a file. Then, Worms are a lot more general, because they can infect documents, spreadsheets, and different files. Thus, once either one enters the system, it will begin replicating itself, infecting networked systems and computers. A good solution to this is by installing anti-malware solutions on all networked devices and systems will considerably scale back the chance of getting these viruses or allowing them to access the system. Through the recognition of the threats early and containing them, these solutions modify admins to notice malicious programs and take them away from them before they get to make any harm to the data.

Secondly, Spyware is any software system that's designed to trace knowledge of your browsing habits and, show the users advertisements and pop-ups. Unlike, Adware collects data together with your consent, and is even supply for corporations since they are able to advertise their products and services, but having advertisements in an excessive amount, it can affect your network’s speed, and even inject malware. Similar to the Drive-By download attacks, these happen when a user enters a website through the browser, and a file or malicious code is downloaded without any consent of the user, infecting the computer and the network, depending on how malicious it is. Keeping your browser up-to-date is one of the most effective ways to assist and establish these malicious sites before you visit them. Also, it is good and recommendable to use a secure search tool, which is designed to filter potential threats and guarantee the user should not navigate to them.

Thirdly, a very damaging type of security threat that is frequently getting used against businesses nowadays is DDoS (Distributed Denial of Service) attacks. The objective of those attacks is to overload the targeted hosted servers with requests of information, creating them inoperable Thus, this type of attacks are often very severe for firms wanting to sell their products and services on-line because it would be inflicting thousands of dollars in lost revenue each day. The first solution to this problem would be the use of WAFs (Web Application Firewalls) since it is a good tool to use against these attacks as the network engineer can add additional management over the network traffic and recognize malicious exploits of requests.

Fourthly, Phishing attacks are a kind of security threat that is designed to steal user logins, bank credentials, and different sorts of personal money info. In most cases, these attacks come from a source replicated as if it was a trustful or popular one. Once you reply to those messages or input your data to these sources, the hacker can use your credentials or enter your money details. In order to prevent these attacks, it is important to check the URLs of the websites or the messages, where the user will be able to verify if the website is actually the real one. Also, train people in a way where they can know what site to access or a message to reply.

Fifthly, Ransomware affects the networks by infecting secure information systems, through encrypting data, and threatening deletion or corruption of files unless the ransom is paid. Ransomware may be a terribly dangerous style of malware. The solutions for this kind of threat are similar to worms and viruses, which are having anti-malware programs that can prevent Ransomware to access the system.

Sixthly, with the increase in the quality of cryptocurrency mining, hackers have found ingenious ways in which of utilizing hardware resources from unsuspecting victims for their gain. They use CriptoJacking where by tricking their victims into loading mining codes onto their computers, hackers will use their CPU and GPU to mine for cryptocurrency, which impacts considerably the performance of their systems. In order to prevent this to happen, the CPU and GPU usage have to be supervised regularly in order to check whether the performance of those is being altered.

Lastly, APTs (Advanced Persistent Threats) are a kind of security threat that consists of wherever an unauthorized associate enters associate unsuspecting system network, the associated remains there for an extended amount undiscovered. instead of inflicting injury to those systems, the associate can quietly sit and steal monetary info and alternative crucial security info. Thus, in order to be protected against this attack, the user must install firewalls, use VPN, and implement intrusion prevention systems, with this the network will have many layers of security.