Network Security

INTRODUCTION

Digitization has transformed our world. How we live, work, play, and learn have all changed. Every organization that wants to deliver the services that customers and employees demand must protect its network.

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources by.

Network security involves the authorization of access to data in a network, which is controlled by the network administration team, a specialized division of IT support team.

Network security is not identifiable with a software or some skilled people, but is a process shared with all company employees.

Network security also helps in protecting proprietary information from attack. Ultimately it protects company reputation.

SECURITY CONCEPTS AND DEVICES

Access control

Not every user should have access to your network. To keep out potential attackers, you need to recognize each user and each device. Then you can enforce your security policies. You can block noncompliant endpoint devices or give them only limited access. This process is network access control (NAC).

Antivirus and antimalware software

"Malware," short for "malicious software," includes viruses, worms, Trojans, ransomware, and spyware. Sometimes malware will infect a network but lie dormant for days or even weeks. The best antimalware programs not only scan for malware upon entry, but also continuously track files afterward to find anomalies, remove malware, and fix damage.

Application security

Any software you use to run your business needs to be protected, whether IT staff builds it or whether you buy it. Unfortunately, any application may contain holes, or vulnerabilities, that attackers can use to infiltrate your network. Application security encompasses the hardware, software, and processes you use to close those holes.

Behavioral analytics

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

Data loss prevention

Organizations must make sure that their staff does not send sensitive information outside the network. Data loss prevention, or DLP, technologies can stop people from uploading, forwarding, or even printing critical information in an unsafe manner.

Email security

Email 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 email security application blocks incoming attacks and controls outbound messages to prevent the loss of sensitive data.

Firewalls
Firewalls put up a barrier between your 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. Similar action is made by a reverse-proxy. Both devices can create a DMZ (demilitarized zone) a physical or logical subnetwork that contains and exposes external-facing services of LAN to a usually larger and untrusted network, usually the Internet or other WAN. The purpose of a DMZ is to add an additional layer of security between LAN and WAN; an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled.

Mobile device security
Cybercriminals are increasingly targeting mobile devices and apps. Within the next 3 years, 90 percent of IT organizations may support corporate applications on personal mobile devices. Of course, companies need to control which devices can access your network and configure their connections to keep network traffic private.

Network segmentation
Software-defined 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. Security standards have to 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.

VPN
A virtual private network encrypts the connection from an endpoint to a network, often over the Internet. Typically, a remote-access VPN uses stardard as IPsec or Secure Sockets Layer to authenticate the communication between device and network.

Web security
A web security solution will control staff’s web use, block web-based threats, and deny access to malicious websites. It will protect web gateway on site or in the cloud. "Web security" also refers to the steps you take to protect your own website.

Wireless security
Wireless networks are not as secure as wired ones. Without stringent security measures, installing a wireless LAN can be like putting Ethernet ports everywhere, including the parking lot. To prevent an exploit from taking hold, security standard needs products specifically designed to protect a wireless network.

ATTACKS
Networks are subject to attacks from malicious sources, they can be from two categories: "*Passive*" when a network intruder intercepts data traveling through the network, and "*Active*" in which an intruder initiates commands to disrupt the network's normal operation or to conduct reconnaissance and lateral movement to find and gain access to assets available via the network.
Some active attacks are: wiretapping, port scanner, idle scan.
Some passive attacks are: Denial-of-service attack, DNS spoofing, Man in the middle, ARP poisoning, VLAN hopping, Smurf attack, Buffer overflow, Heap overflow, Format string attack, SQL injection, Cross-site scripting, CSRF,Cyber-attack.
Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access.

The term "social engineering" as an act of psychological manipulation is also associated with the social sciences, but its usage has caught on among computer and information security professionals. All social engineering techniques are based on specific attributes of human decision-making known as cognitive biases exploited in various combinations to create attack techniques, some of which are listed below.

- *Pretexting*
- *Diversion theft*
- *Phishing*
- *Baiting*
- *Quid pro quo*
- *Tailgating*

The attacks used in social engineering can be used to steal employees' confidential information. The most common type of social engineering happens over the phone. Other examples of social engineering attacks are criminals posing as exterminators, fire marshals and technicians to go unnoticed as they steal company secrets.

The most notable social engineer was hacker Kevin Mitnik, a reformed computer criminal and later security consultant who points out that it is much easier to trick someone into giving a password for a system than to spend the effort to crack into the system.