LECTURE NOTE 3 [CSC 421]

NETWORK SECURITY

A network is a collection of devices, such as computers, servers, and printers, connected to share information and resources. A network consists of two or more computers that are linked to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

3.1 Network Security

Network security is a term that describes the security tools, tactics, and security policies designed to monitor, prevent, and respond to unauthorized network intrusion, while also protecting digital assets, including network traffic.

Network security includes hardware and software technologies (including resources such as savvy security analysts, hunters, and incident responders). It is designed to respond to the full range of potential threats targeting your network.

Network security is the defense you use to protect yourself against ever-increasing cybercrime.

3.2 The Three Key Focuses of Network Security

Three key focuses should serve as a foundation of any network security strategy: protection, detection, and response.

- ***Protection*** entails any tools or policies designed to prevent network security intrusion.
- ***Detection*** refers to the resources that allow you to analyze network traffic and quickly identify problems before they can cause harm.
- ***Response*** is the ability to react to identified network security threats and resolve them as quickly as possible.

3.3 Benefits of Network Security

Network security tools and devices enable organizations to protect their sensitive information, overall performance, reputation, and continuity in business.

Secure and reliable networks protect not just organizational interests and operations, but also any client or customer who exchanges information with the organization, in addition to the general public.

The benefits of network security are:

1. Builds trust

Security for large systems translates to security for everyone. Network security boosts client and consumer confidence, and it protects your business from the reputational and legal fallout of a security breach.

2. Mitigates risk

The right network security solution will help your business stay compliant with business and government regulations, and it will minimize the business and financial impact of a breach if it does occur.

3. Protects proprietary information

Your clients and customers rely on you to protect their sensitive information. Your business relies on that same protection, too. Network security ensures the protection of information and data shared across the network.

4. Enables a more modern workplace

From allowing employees to work securely from any location using VPN to encouraging collaboration with secure network access, network security provides options to enable the future of work. Effective network security also provides many levels of security to scale with your growing business.

3.4 Network Security Tools and Techniques

Enterprises' networks encounter varying degrees of threats and therefore should be prepared to defend, identify, and respond to a full range of attacks. However, the reality is that the biggest danger to most companies is not fly-by-night threat actors, but the attackers that are well-funded and are targeting specific organizations for specific reasons. Hence, network security strategy needs to be able to address the various methods these actors might employ.

Here are 14 different network security tools and techniques designed to help you do just that:

1) **Access control:** If threat actors cannot access your network, the amount of damage they will be able to do will be extremely limited. But in addition to preventing unauthorized access, be aware that even authorized users can be potential threats. Access control allows you to increase your network security by limiting user access and resources to only the parts of the network that directly apply to individual users' responsibilities.

2) **Anti-malware software:** Malware, in the form of viruses, trojans, worms, keyloggers, spyware, etc. is designed to spread through computer systems and infect networks. Anti-malware tools are a kind of network security software designed to identify dangerous programs and prevent them from spreading. Anti-malware and antivirus software may also be able to help resolve malware infections, minimizing the damage to the network.

3) **Anomaly detection:** It can be difficult to identify anomalies in your network without a baseline understanding of how that network should be operating. Network anomaly detection engines (ADE) allow you to analyze your network so that when breaches occur, you will be alerted to them quickly enough to be able to respond.

4) **Application security:** For many attackers, applications are a defensive vulnerability that can be exploited. Application security helps establish security parameters for any applications that may be relevant to your network security.

5) **Data Loss Prevention (DLP):** Often, the weakest link in network security is the human element. DLP technologies and policies help protect staff and other users from misusing and possibly compromising sensitive data or allowing said data out of the network.

6) **Email security:** As with DLP, email security is focused on shoring up human-related security weaknesses. Via phishing strategies (which are often very complex and convincing), attackers persuade email recipients to share sensitive information via desktop or mobile device, or inadvertently download malware into the targeted network. Email security helps identify dangerous emails and can also be used to block attacks and prevent the sharing of vital data.

7) **Endpoint security:** The business world is becoming increasingly, "bring your own device" (BYOD), to the point where the distinction between personal and business computer devices is almost non-existent. Unfortunately, sometimes personal devices become targets when users rely on them to access business networks. Endpoint security adds a layer of defense between remote devices and business networks.

8) **Firewalls:** Firewalls function much like gates that can be used to secure the borders between your network and the internet. Firewalls are used to manage network traffic, allowing authorized traffic through while blocking access to non-authorized traffic.

9) **Intrusion prevention systems:** Intrusion prevention systems (also called intrusion detection) constantly scan and analyze network traffic/packets, so that different types of attacks can be identified and responded to quickly. These systems often keep a database of known attack methods, to be able to recognize threats immediately.

10) **Network segmentation:** There are many kinds of network traffic, each associated with different security risks. Network segmentation allows you to grant the right access to the right traffic while restricting traffic from suspicious sources.

11) **Security information and event management (SIEM)**: Sometimes simply pulling together the right information from so many different tools and resources can be prohibitively difficult — particularly when time is an issue. SIEM tools and software give responders the data they need to act quickly.

12) **Virtual private network (VPN):** VPN tools are used to authenticate communication between secure networks and an endpoint device. Remote-access VPNs generally use IPsec or Secure Sockets Layer (SSL) for authentication, creating an encrypted line to block other parties from eavesdropping.

13) **Web security:** Including tools, hardware, policies, and more, web security is a blanket term to describe the network security measures businesses take to ensure safe web use when connected to an internal network. This helps prevent web-based threats from using browsers as access points to get into the network.

14) **Wireless security:** Generally speaking, wireless networks are less secure than traditional networks. Thus, strict wireless security measures are necessary to ensure that threat actors are not gaining access.