Part 1: A

In today's digitally-driven world, computer networks have become an essential component of any organization's infrastructure. With the increase in the use of the internet and cloud computing, the security of computer networks has become a major concern for all types of organizations. Cybersecurity has become a critical issue for businesses, governments, and individuals alike. In this context, computer networks play a crucial role in cyber security, as they provide a platform for secure communication and information exchange. In this article, we will discuss the importance of computer networks in cyber security.

Computer networks provide a platform for the exchange of information between different users and devices (*Computer Networks* ). This information may include sensitive data such as personal information, financial data, or confidential business data. To ensure that this information is secure, computer networks use various security protocols and encryption techniques to protect the data from unauthorized access. Network Security, Firewalls, and VPNs) This is particularly important for businesses that rely on the exchange of confidential data with their customers, partners, or suppliers.

Computer networks play a critical role in detecting and preventing cyber attacks (Mohanakrishnan, R., 2022). With the use of advanced intrusion detection and prevention systems, computer networks can detect and respond to cyber attacks in real-time. This helps organizations to identify and respond to security threats before they cause any damage.

With the increasing popularity of remote work, computer networks have become a critical component of remote access. Remote access allows employees to access the company's network and resources from anywhere in the world (*Secure remote access: What it is and how it works*. ). However, this also increases the risk of cyber attacks, as remote access is often done through unsecured networks. To mitigate this risk, computer networks use various security protocols such as Virtual Private Networks (VPNs) to provide secure remote access.

They also provide a centralized platform for managing and controlling access to resources. This makes it easier for organizations to enforce security policies and ensure that users only have access to the resources they need. Centralized management also makes it easier to monitor and track user activity, which is essential for detecting and preventing security breaches.

In the event of a cyber attack or a system failure, organizations need to be able to recover their data quickly and efficiently. Computer networks provide a platform for backing up and recovering data, which is essential for maintaining business continuity.

Computer networks are scalable, which means they can adapt to changing business needs. As organizations grow, they need to add new users, devices, and applications to their network. Computer networks can easily accommodate these changes, while ensuring that security is not compromised.

In conclusion, computer networks play a critical role in cyber security. They provide a platform for secure communication and information exchange, enable the detection and prevention of cyber attacks, provide secure remote access, offer centralized management, facilitate data backup and recovery, and are scalable to meet changing business needs. With the increasing threat of cyber attacks, it is essential for organizations to invest in robust computer networks that are designed with security in mind.

***Bibliography***

Auburn IT - Information Technology Service Provider. (n.d.). *The importance of Computer and Network Security*. Auburn IT. Retrieved April 25, 2023, from https://www.auburnit.com/news/26-the-importance-of-computer-and-network-security

Kent, K., Scarfone, K., & Mell, P. (2014). *Guide to intrusion detection and prevention systems (idps): Recommendations of the National Institute of Standards and Technology*. U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology.

Kotenko, I., & Skormin, V. A. (2010). *Computer Network Security: 5th International Conference on Mathematical Methods, models and architectures for computer network security, Mmm-Acns 2010, St. Petersburg, Russia, September 8-10, 2010: Proceedings*. Springer.

*Secure remote access: What it is and how it works*. business.com. (n.d.). Retrieved April 25, 2023, from https://www.business.com/articles/secure-remote-access/

Specialist, R. M. I. T., Mohanakrishnan, R., Specialist, I. T., 11, L. U. F., Ramya Mohanakrishnan is an IT specialist who has worked in the startup industry for more than a decade. She has coded. (2022, February 11). *What is intrusion detection and prevention system? definition, examples, techniques, and best practices*. Spiceworks. Retrieved April 25, 2023, from https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-idps/

Stewart, J. M., & Kinsey, D. (2021). *Network security, firewalls, and Vpns*. Jones & Bartlett Learning.

*What is network security and why is it important?* Herzing University. (2022, January 11). Retrieved April 25, 2023, from https://www.herzing.edu/blog/what-network-security-and-why-it-important

Wikipedia, with help from B. P. (n.d.). *Computer Networks*. Information People and Technology. Retrieved April 25, 2023, from https://psu.pb.unizin.org/ist110/chapter/2-2-computer-networks/

Yasar, K., & Gillis, A. S. (2023, March 28). *What is a computer network?: Definition from TechTarget*. Networking. Retrieved April 25, 2023, from https://www.techtarget.com/searchnetworking/definition/network

Part 1: B) Types of Networks:

1. LAN (Local Area Network): This is a network that covers a small area, such as an office, building, or campus. It is usually owned and managed by a single organization.
2. WAN (Wide Area Network): This is a network that covers a large geographic area, such as a city, state, or country. It is typically used to connect multiple LANs or other networks together.
3. MAN (Metropolitan Area Network): This is a network that covers a larger area than a LAN but smaller than a WAN, typically a city or metropolitan area.
4. WLAN (Wireless Local Area Network): This is a type of LAN that uses wireless technology to connect devices to the network.
5. PAN (Personal Area Network): This is a network that connects devices within a single person's workspace, such as a computer, phone, and other portable devices.

Part 1: C) Network Topologies:

1. Star Topology: In this topology, all devices are connected to a central hub or switch. This makes it easy to add or remove devices from the network.
2. Bus Topology: In this topology, all devices are connected to a central cable called a bus. Data is transmitted along the cable, and devices receive the data that is relevant to them.
3. Ring Topology: In this topology, devices are connected in a circular fashion, with each device connected to the device next to it. Data is transmitted around the ring until it reaches its destination.
4. Mesh Topology: In this topology, each device is connected to every other device on the network. This provides redundancy and ensures that the network remains operational even if one or more devices fail.
5. Hybrid Topology: This is a combination of two or more topologies, such as a star-bus or ring-mesh topology.

Part 1 D) Networking Devices:

1. Routers: Routers are used to connect multiple networks together and to route data between them. They also provide security features such as firewalls and access control.
2. Switches: Switches are used to connect devices within a network and to direct data traffic to its destination.
3. Hubs: Hubs are used to connect devices within a network, but they are less intelligent than switches and do not direct data traffic to its destination.
4. Firewalls: Firewalls are used to protect a network from external threats by monitoring incoming and outgoing traffic and blocking traffic that is not authorized.

Part 2: A) Network Scan Results:

After performing a basic network scan on the company's network, several potential security vulnerabilities were identified. These include:

Unpatched Operating Systems: Several systems within the network were found to be running outdated versions of the operating system. This could allow hackers to exploit known vulnerabilities and gain unauthorized access to the network.

Weak Passwords: Many user accounts within the network were found to have weak passwords. This makes it easy for hackers to guess passwords and gain access to the network.

Unsecured Wireless Network: The wireless network was found to be unsecured, meaning that anyone can connect to the network without a password. This makes it easy for hackers to access the network and steal sensitive information.

Lack of Firewall Protection: The network was found to be lacking proper firewall protection. This means that it is more vulnerable to external attacks and data breaches.

Part 2 B) Measures to Secure the Network:

To secure the network and prevent future attacks, the following measures are recommended:

Regular Patching: The company should ensure that all operating systems and applications are regularly patched to fix any known vulnerabilities.

Strong Password Policies: The company should enforce strong password policies, including requiring users to use complex passwords and changing them regularly.

Securing the Wireless Network: The company should secure the wireless network by using WPA2 encryption and creating a strong password. It is also recommended to set up a separate guest network for visitors to use.

Firewall Protection: The company should implement a firewall to protect the network from external attacks.

Part 2 C) Plan to Monitor and Maintain Network Security:

To maintain the security of the network, the following plan is recommended:

Regular Scanning: The network should be regularly scanned for vulnerabilities and security risks.

Security Updates: Operating systems, applications, and firmware should be regularly updated to ensure that they are secure.

User Awareness: The company should provide regular training to employees to increase their awareness of cybersecurity risks and best practices.

Incident Response Plan: The company should develop an incident response plan to ensure that they can respond quickly and effectively to any security breaches.