NETWORK INFRASTRUCTURE SECURITY

Nakyejjwe Flavia
Nanyanzi Deborah

Nalubwama Christine

Network security

Network Security is a process of protecting the underlying networking infrastructure by installing preventative measures to deny unauthorized access, modification, deletion, and theft of resources and data

Infrastructure security is the practice of protecting critical systems and assets against physical and cyber threats.

Types of network security

Access Control: The prevention of unauthorized users and devices from accessing the network.

Email security: Here, processes, products, and services are designed to protect your email accounts and email content safe from external threats.

Firewalls: This controls incoming and outgoing traffic on networks, with predetermined security rules.Gatekeeping devices that can allow or prevent specific traffic from entering or leaving the network are used here.

Virtual Private Networks (VPN): VPNs encrypt connections between endpoints creating a secure “tunnel” of communications over the internet.

Behavioral Analytics: These tools automatically detect network activity that deviates from usual activities.

Wireless Security: Wireless networks are less secure than hardwired networks, and with the proliferation of new mobile devices and apps, there are ever-increasing vectors for network infiltration.

Why is Network and Infrastructure Security important?

- To protect your data. It is essential to protect your organization’s data from theft, corruption, or loss.
- To ensure continuity of operations. In the event of a natural disaster, a well-protected network infrastructure can help ensure that your business can continue to operate smoothly. This can be inform of using reliable backup solutions.
- To meet compliance requirements. Many industries have strict compliance requirements when it comes to data security. By investing in appropriate network security measures, you can help ensure that your organization meets all relevant regulations.
- To protect your reputation. In cases of security breach, can spread quickly and damage your organization’s reputation..

Threats to network and infrastructure security

1.Unauthorized Access: When users gain access to systems or networks without proper authorization, it can lead to data breaches and other security incidents.

2.Natural Disasters: Physical infrastructure can be damaged or destroyed by natural events, disrupting network operations and potentially leading to data loss.

3.Shadow IT: Employees using unauthorized or unmonitored applications and services can introduce security vulnerabilities.

4.Lack of Security Updates: Failing to apply security patches and updates can leave systems susceptible to known vulnerabilities.

5.Misconfigurations: Incorrectly configured security settings can leave systems and networks vulnerable to attacks.

6.Data Theft: Stealing sensitive data, either during transit or while stored, is a constant threat.

7.Malware: Malicious software, such as viruses, worms, Trojans, and ransomware, can infect systems and compromise network security.

8.Phishing: Phishing attacks use deceptive emails, websites, or messages to trick users into revealing sensitive information like login credentials or financial details.

Measures taken to improve network and infrastructure security

There are a number of steps that organizations can take to improve their network infrastructure security, including:

1. Implementing strong authentication and authorization controls.
2. Encrypting sensitive data.
3. Deploying intrusion detection and prevention systems.
4. Conducting regular security audits and vulnerability assessments.
5. Limit unnecessary lateral communications: Unfiltered communication between peers could allow intruders to move about freely from computer to computer.This is mainly in the peer-to-peer communications within a network
6. Harden network devices: Hardening network devices is a primary way to enhance network infrastructure security. It is advised to adhere to industry standards and best practices regarding network encryption,
7. Secure access to infrastructure devices: Administrative privileges are granted to allow certain trusted users access to resources.
8. Validate integrity of hardware and software: Organizations should regularly perform integrity checks on their devices and software.

Benefits of Network Infrastructure Security?

Improved resource sharing saves on costs: Due to protection, resources on the network can be utilized by multiple users without threat, ultimately reducing the cost of operations.

Shared site licenses: Security ensures that site licenses would be cheaper than licensing every machine.

File sharing improves productivity: Users can securely share files across the internal network.

Internal communications are secure: Internal email and chat systems will be protected from prying eyes.

Compartmentalization and secure files: User files and data are now protected from each other, compared with using machines that multiple users share.

Data protection: Data backup to local servers is simple and secure, protecting vital intellectual property.