In this assignment, you will research and analyze different types of cyberattacks that target the availability of systems, networks, or data, which is one of the core principles of cybersecurity. Known as "Attacks on Availability," these are incidents where malicious actors attempt to disrupt access to critical resources, making them inaccessible to users. Such attacks can include Distributed Denial of Service (DDoS), ransomware, and other forms that focus on hindering legitimate access.

Objective: You are tasked with providing a concise, **250-word** summary of a specific attack on availability. Use recent online sources to explore how these attacks occur, their impact on organizations, and possible defenses. Be sure to cite at least one reputable source to support your analysis.

In your response, address the following:

- Define what is meant by an "attack on availability."
- Describe a recent example of such an attack or a common technique used in these attacks.
- Briefly discuss the broader implications of these attacks on organizations and users.

An attack on availability is a type of attack that targets computer systems. Its main objective is to cause the systems to become unavailable to a user. These types of attacks involve cyberattacks on the internet. An example of this type of attack is a distributed denial of service attack. Also known as a “DDoS” attack. These attacks usually involve one person or multiple people who can block access to a database, computer, and other devices connected to the network. During these attacks hackers will send network traffic and packets to any device that is connected to the network. On February 27, 2017, Amazon Web Services experienced an outage that resulted in many users losing access to the system and also losing the function of being able to control the functionality of devices connected to the network. In July 2001, the company Microsoft suffered an attack that shut down tens of thousands of machines within the company. This attack occurred two months before the unfortunate event that occurred in New York City, also known as 9/11. The most effective way to defend against these attacks is to implement a defense strategy. Investing in a managed service provider (MSP) allows a company’s network to be closely monitored and allows it to mitigate attacks. If an attack were to occur, the service provider is to make adjustments and respond to the attack right away. The service provider enables the company to have an enhanced security system and provide leverage against cyberattacks.

Sources

Availability attack. Availability Attack - an overview | ScienceDirect Topics. (n.d.). https://www.sciencedirect.com/topics/computer-science/availability-attack

Canada, C. S. E. (2024, February 23). *Defending against distributed denial of service (ddos) attacks – itsm.80.110*. Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/guidance/defending-against-distributed-denial-service-ddos-attacks-itsm80110

Imi. (2021, April 24). *Cyber attack methods on internet availability*. Identity Management Institute®. https://identitymanagementinstitute.org/cyber-attack-methods-on-internet-availability/