Module 1: Cybersecurity Threats, Vulnerabilities & Attacks

Endpoint Security | Cisco Networking Academy

Prepared by: Kudzaishe Majeza

Agenda

- Introduction to Cybersecurity
- Understanding Threats
- Vulnerabilities in Systems & Users
- Types of Cyber Attacks
- Threat Actors & Their Motivations
- Attack Techniques
- Defense & Prevention Strategies
- Summary

Real-Life Current Cybersecurity Attack Example

One of the most significant recent incidents was the **2024 Change Healthcare ransomware attack**. The attack, carried out by the ALPHV/BlackCat ransomware group, disrupted healthcare services all over the United States. Hospitals were unable to process payments, pharmacies couldn’t verify insurance, and patient data was potentially exposed. The attack cost hundreds of millions of dollars and demonstrated how a single vulnerability in one endpoint or system can cascade into a nationwide crisis.

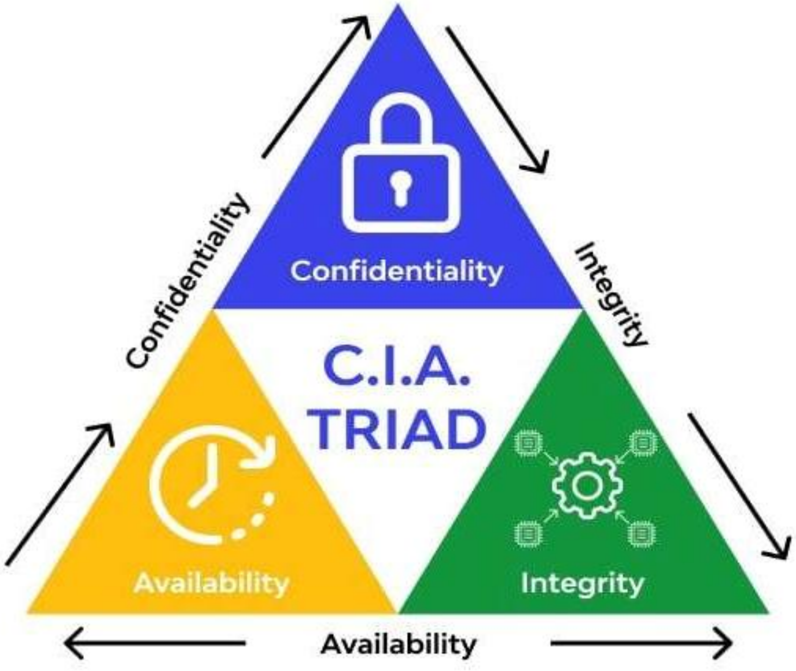
- This example fits perfectly with the module because it includes:
- A real threat actor (ransomware gang)
- A vulnerability that was exploited
- An attack that compromised availability and potentially confidentiality

Introduction to Cybersecurity

- Cybersecurity protects data, users, and systems.
- Endpoints are the most common attack targets.
- Understanding threats helps build strong defenses.
- The CIA triad: Confidentiality, Integrity, Availability.

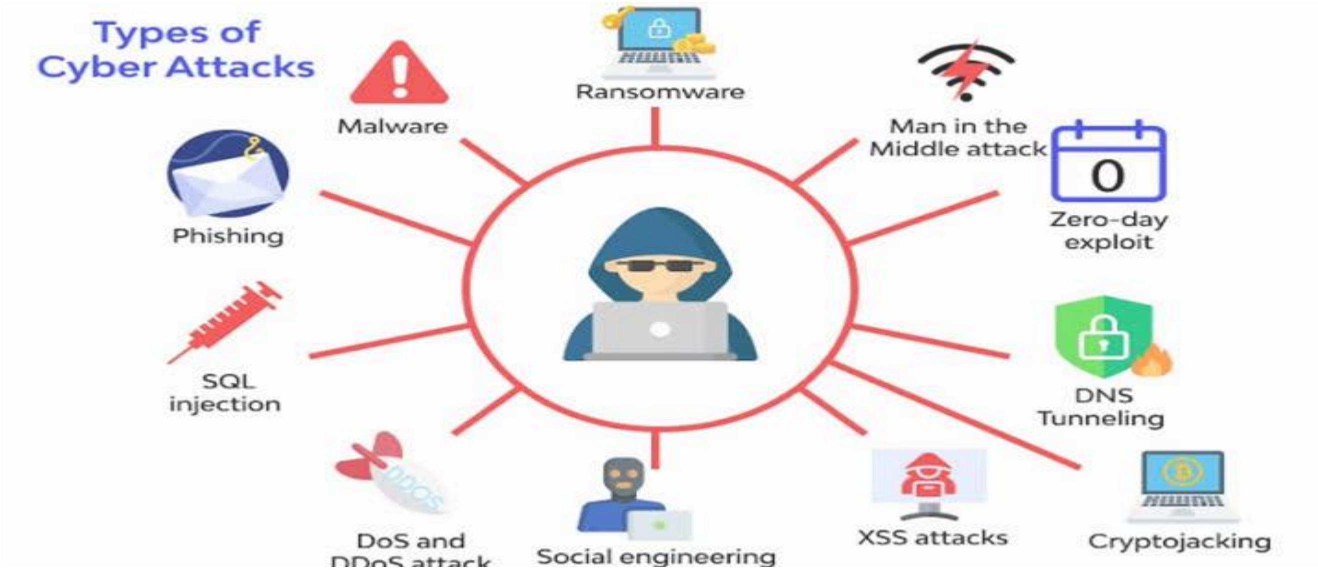
The CIA Triad

- Confidentiality – Protect information from unauthorized access.
- Integrity – Ensure data is not altered or tampered with.
- Availability – Ensure systems and data are accessible when needed.



Cybersecurity Threats

- Malware (viruses, worms, Trojans, spyware, ransomware)
- Phishing and social engineering
- Insider threats (malicious or accidental)
- Zero-day threats
- Supply-chain attacks
- Advanced Persistent Threats (APTs)



Cybersecurity Vulnerabilities

- Weak authentication methods
- Poor software patching
- Misconfigured firewalls & ACLs
- Lack of physical security controls
- Social engineering susceptibility
- Insecure network protocols

Human Vulnerabilities

- Falling for phishing emails
- Reusing passwords across platforms
- Weak or predictable passwords
- Plugging unknown USB devices
- Sharing credentials unintentionally

Types of Cyber Attacks

- Ransomware attacks
- Credential theft & keylogging
- SQL injection & web-based attacks
- Distributed Denial of Service (DDoS)
- Man-in-the-Middle (MITM)
- Exploit-based attacks (buffer overflow, remote code execution)

Threat Actors

- Cybercriminals seeking financial gain
- Hacktivists motivated by ideology
- Nation-state groups for espionage & disruption
- Organized cyber gangs
- Insiders with privileged access

Common Attack Techniques

- Social engineering deception
- Exploiting unpatched software flaws
- Password cracking (brute force, dictionary attacks)
- Malware delivery via email or downloads
- MITM interception of data
- Privilege escalation attacks

Defense & Prevention Strategies

- Implement endpoint protection platforms (EPP/EDR)
- Enforce MFA and strong password policies
- Regular OS and application patching
- Network segmentation & least-privilege access
- Continuous monitoring & logging
- User security awareness training

Summary

- Threats, vulnerabilities, and attacks evolve constantly.
- Endpoints remain a primary focus for attackers.
- Understanding threats is the first step in defense.
- Layered security strategies significantly reduce risk.