Marina Khoshaba

12/23/25

Cybersecurity Foundations: Threats, CIA Triad, and Common Attacks

Cybersecurity aids in protecting systems, networks, and data from unauthorized access and attacks. Organizations become targets as they rely more on digital infrastructure. Understanding security concepts such as threats, CIA Triad, and common attack types is essential in maintaining secure systems and protecting sensitive information.

Cybersecurity threats are any potential actions that can cause harm to computer systems, networks, or any data by comprising confidentiality, integrity, or availability. Threats can be intentional such that a hacker is launching an attack or even accidental such as an employee clicking a malicious link. Some examples of cybersecurity threats include malware, insider threats, external attackers, and phishing. Malware is a malicious software like viruses or ransomware designed to damage systems or steal information. Insider threats are where employees or trusted users misuse their access either accidentally or intentionally. External attackers are hackers or cybercriminals attempting to gain access to systems from outside the organization. Phishing uses deceptive emails to trick users into revealing sensitive information. Many of these threats succeed because they exploit existing vulnerabilities in systems, software, or human behavior.

The CIA Triad is a foundational model in cybersecurity that represents the three principles to protect information systems: Confidentiality, Integrity, and Availability. Most security polices, controls, and technologies support one or more of these principles. Confidentiality ensures that information is accessible only to authorized individuals and systems, Its primary goal is to prevent unauthorized access, disclosure, or data leaks. Common methods used to maintain confidentiality include encryption that scrambles data and access controls which requires multi-factor authentication. A popular example of confidentiality is online banking where customer's data is encrypted, so attackers are unable to read it without proper credentials. Integrity focuses on ensuring that the data used is accurate, complete, and unaltered unless modified. This protects systems from unauthorized changes, whether caused by attackers, software bugs, or accidental user errors. Hashing and checksums are used to verify data integrity by detecting changes to files or messages. Availability ensures that systems, services, and data are accessible when needed by authorized users. Even if data is secure and accurate, it is useless if it cannot be accessed. Organizations maintain availability through backups and protection against denial-of-service attacks. Confidentiality, integrity, and availability form the backbone of effective cybersecurity strategies.

Common cyber-attacks are methods used to exploit vulnerabilities in systems, networks, or users. One of the most common attacks is phishing, which involves deceptive emails or messages designed to trick users into revealing sensitive information such as passwords or credit card

numbers. Phishing is dangerous because it targets human behavior rather than technical flaws. Basic prevention includes user awareness training and email filtering. Malware refers to malicious software such as viruses, worms, spyware, and ransomware. Malware can steal data, disrupt systems, or encrypt files for ransom. It's dangerous due to how quickly it can spread and cause significant damage. Some prevention methods include antivirus software, system updates, and cautious downloading practices. Denial-of-Service attack attempts to overwhelm a system with excessive traffic making it unavailable to legitimate users. Organizations defend against DoS attacks using traffic monitoring, rate limiting, and redundant infrastructure. A man in the middle attack occurs when an attacker intercepts communication between two parties without their knowledge. This can lead to data theft or manipulation. Using secure connections such as https and encrypted Wi-Fi networks help prevent these attacks. Password attacks, including both brute force and credential stuffing, aim to gain unauthorized access by guessing or reusing passwords. Using strong, unique passwords and multi-factor authentication are effective prevention techniques.

Cybersecurity fundamentals such as the CIA Triad and common attack methods form the foundation of all secure systems. Understanding these concepts help individuals and organizations recognize risks, protect sensitive data, and respond effectively to threats. Security awareness is especially important because many successful attacks exploit human behavior rather than technical weaknesses alone. As technology continues to evolve, applying these core principles ensures that real world systems remain secure, reliable, and resilient against both current and emerging cyber threats.