CONCEPTS OF CYBERSECURITY

SAVANNAH STATE UNIVERSITY

GENCYBER - SUMMER CAMP 2024

ENGINEERING TECHNOLOGY DEPARTMENT
SAVANNAH STATE UNIVERSITY

SSU-GENCYBER TEAM

Mr. Alberto De La Cruz, Assistant Professor and PI
Dr. Mir Hayder, Professor and Co-PI
Mrs. Theresa Luciano, Oglethorpe Charter Teacher/Instructor
Mrs. Veronica De La Cruz, RHMS Teacher/Instructor

Defense in Depth

Defense in Depth is a cybersecurity strategy that involves implementing multiple layers of security controls to protect against various threats. It recognizes that relying on a single security measure is insufficient and emphasizes the use of complementary security measures across different layers of an information system.

Example 1: Implementing firewalls, intrusion detection systems (IDS), and antivirus software to secure the network perimeter.

Example 2: Using access controls, authentication mechanisms, and encryption to protect sensitive data within the network.

Confidentiality

Confidentiality ensures that information is accessible only to authorized individuals or systems. It involves protecting sensitive data from unauthorized access, disclosure, or theft. Encryption, access controls, and data classification are commonly used to enforce confidentiality.

Example 1: Encrypting sensitive data stored in databases or transmitted over networks to prevent unauthorized access.

Example 2: Implementing access controls and user authentication to restrict access to confidential files and documents.

Integrity

Integrity ensures that data remains accurate, complete, and unaltered. It involves implementing mechanisms to detect and prevent unauthorized modifications or tampering of data. Techniques such as digital signatures, checksums, and secure hash algorithms are used to verify data integrity.

Example 1: Using digital signatures to verify the authenticity and integrity of important documents and files.

Example 2: Implementing checksums or hash algorithms to detect any unauthorized modifications or tampering of data.

Availability

Availability ensures that systems, resources, and data are accessible and usable when needed. It involves protecting against disruptions or service outages caused by various factors, including cyber attacks, hardware failures, or natural disasters. Redundancy, backup systems, and disaster recovery plans are used to maintain availability.

Example 1: Implementing redundancy and backup systems to mitigate the impact of hardware failures or system crashes.

Example 2: Developing and testing disaster recovery plans to quickly restore operations after a cyber incident or natural disaster.

Think Like an Adversary

This concept encourages individuals to adopt a proactive mindset by thinking like a potential adversary. By understanding the motivations, techniques, and tactics employed by attackers, individuals can better anticipate and mitigate potential cyber threats. It promotes a proactive approach to identify vulnerabilities, implement appropriate security measures, and stay one step ahead of potential adversaries.

Example 1: Conducting penetration testing or ethical hacking to identify vulnerabilities in systems and applications.

Example 2: Staying updated with the latest cybersecurity news and trends to proactively respond to emerging threats.

Keep it simple

This concept emphasizes the importance of simplicity and avoiding unnecessary complexities in cybersecurity practices. It encourages individuals to focus on implementing robust and effective security measures while avoiding unnecessary complexity that could introduce additional vulnerabilities or hinder proper security management.

Example 1: Regularly updating software and operating systems to patch known vulnerabilities.

Example 2: Providing cybersecurity training and awareness programs to educate employees about common threats and best practices.

Questions?