Durna, Jerome T.
BSIT-31008

WEEK 13 - Cybersecurity Threats

Preliminary
Question: Why is it important to understand different types of cybersecurity threats, and how can awareness of these threats help individuals and organizations protect their data?

Answer: Understanding different types of cybersecurity threats is essential because it helps both individuals and organizations recognize potential dangers before they cause harm. Awareness allows people to take preventive measures, such as using strong passwords, installing antivirus software, and avoiding suspicious links. When everyone knows how these threats work—like viruses, phishing, or hackers—they can act responsibly online, reducing the chances of data loss, identity theft, or system damage. In short, cybersecurity awareness builds a stronger digital defense and promotes a safer online environment for everyone.

Identification
1. Question: Malware that replicates to damage computer files.

   Answer: Computer Virus

2. Question: Attempt to steal personal data by masquerading as a trusted entity.

   Answer: Phishing

3. Question: Unauthorized access to data by exploiting systems.

   Answer: Hacker

4. Question: Program that tracks online activities without consent.

   Answer: Spyware

5. Question: Data being transferred across a network.

   Answer: Data in Motion

6. Question: Data that is stored and not currently in use.

   Answer: Data at Rest

7. Question: Antivirus feature that protects against unauthorized access.

   Answer: Firewall

8. Question: Data actively being accessed or used by the system.

Answer: Data in Use

9. Question: Data protection by monitoring network traffic.

Answer: Identity Theft Protection

10. Question: Software that detects and removes malicious programs.

Answer: Antivirus Software

Generalization
Question: Explain the importance of protecting data at rest, data in use, and data in motion, and describe at least one security measure for each type of data.

Answer: Protecting data at rest, data in use, and data in motion is crucial to maintaining information security. Data at rest refers to stored information, such as files on a hard drive or database, which can be protected through encryption and secure storage. Data in use is information currently being processed by a system, which can be secured by access controls and authentication to prevent unauthorized access. Meanwhile, data in motion is information being transmitted over networks, best protected by firewalls and VPN encryption. Together, these security measures safeguard data throughout its entire lifecycle.

Evaluation (Multiple Choice)
1. Question: What type of malware is designed to replicate and damage systems?

Answer: a. Computer virus

2. Question: What can hackers compromise if they gain unauthorized access to a system?

Answer: b. Sensitive information like credit card data

3. Question: Which tool can help protect against spyware?

Answer: d. Antivirus software with internet security features

4. Question: Which of the following is crucial to avoid computer viruses?

Answer: b. Evaluating free downloads carefully

5. Question: What is the primary characteristic of a computer virus?

Answer: c. It modifies computer operation without user permission

6. Question: Phishing is most commonly conducted through?

Answer: c. Emails and instant messages

7. Question: Which is the best defense against online predators?

Answer: b. Antivirus with identity theft protection

8. Question: Why is up-to-date antivirus software essential?

Answer: b. It protects against the latest security threats

9. Question: When data is loaded into memory for a program to run, it is considered?

Answer: a. Data in Use

10. Question: Which action can help reduce the risk of phishing?

Answer: d. Using antivirus software with identity theft protection

Assignment (True/False)

1. Question: Data at rest refers to data that is currently being transferred over a network.

Answer: False

2. Question: Spyware is a type of malware that monitors a user's online activities without their knowledge.

Answer: True

3. Question: Phishing attacks typically aim to steal sensitive information by impersonating a trusted entity.

Answer: True

4. Question: A firewall helps protect against computer viruses by scanning files for malicious code.

Answer: False

5. Question: Data in use is information that resides in memory and is actively being processed by a computer system.

Answer: True

WEEK 14 - Authentication and Authorization

Preliminary

Question: Why is it essential for organizations to implement both authentication and authorization processes in their computer systems? Describe how these processes contribute to the overall security of data within the system.

Answer: It is essential for organizations to implement both authentication and authorization to ensure that only legitimate users access sensitive data and systems.

Authentication verifies the user's identity—such as through passwords, fingerprints, or ID cards—while authorization determines what actions or data that user is allowed to access. Together, they prevent unauthorized users from viewing or altering information. Without these processes, organizations risk data breaches and misuse of resources. These mechanisms form the foundation of secure digital operations, ensuring data integrity and privacy for all users.

Identification

1. Question: Automatic execution of code from a removable drive

   Answer: Maintenance Phase

2. Question: Process of verifying identity with credentials

   Answer: Authentication

3. Question: Ensuring user has permissions for actions

   Answer: Authorization

4. Question: An example of 'something you know'

   Answer: Password

5. Question: Weakness in a system's security

   Answer: Design Vulnerability

6. Question: Using fingerprint or Iris for identity

   Answer: Biometric Factor

7. Question: An example of 'something you have'

   Answer: Token Generator

8. Question: Verifies identity with 'something you are'

   Answer: Biometric Factor

9. Question: Data stored on USB or hard drive, not actively used

   Answer: Data at Rest

10. Question: Attempt to steal data through fraudulent messages

    Answer: Phishing

Generalization

Question: Explain the difference between authentication and authorization and provide an example of how each process is used to protect data in an organization's computer

system. Additionally, discuss one potential vulnerability that could compromise either authentication or authorization and how it might be mitigated.

Answer: Authentication and authorization are both key processes in protecting digital data. Authentication ensures a user is who they claim to be—often through passwords, PINs, or biometrics—while authorization decides what that verified user can access, like viewing records or modifying data. For example, an HR employee may be authenticated through a password but authorized only to view certain employee files. A vulnerability that can compromise these processes is weak password security, which can be mitigated through multi-factor authentication (MFA) and strong password policies. Together, they strengthen the entire security system.

Evaluation (Multiple Choice)

1. Question: A vulnerability that occurs due to programming mistakes is most likely introduced during which phase?

   Answer: b. Implementation

2. Question: What type of vulnerability does a lack of access control introduce?

   Answer: d. Design vulnerability

3. Question: In which phase can a security vulnerability arise if security requirements are not identified?

   Answer: a. Analysis

4. Question: Which of the following can result from an input validation flaw?

   Answer: a. Arbitrary code execution by attackers

5. Question: Which of these is a weakness that can allow attackers to exploit a system?

   Answer: b. Vulnerability

6. Question: Leaving a default password unchanged is an example of a vulnerability in which phase?

   Answer: d. Deployment

7. Question: What is the primary risk of using a simple or default password?

   Answer: b. It introduces a vulnerability during deployment

8. Question: Which of the following is an example of a biometric authentication factor?

   Answer: b. Iris scan

9. Question: Which authentication factor might be compromised if the user loses a token generator?

Answer: a. Something the user has

10. Question: In information security, authorization follows:

Answer: c. Authentication

Assignment (True/False)

1. Question: Authentication is the process of verifying a user's identity, while authorization determines the user's permissions.

Answer: True

2. Question: Using only one authentication factor is more secure than using multiple factors.

Answer: False

3. Question: Vulnerabilities in a system can be introduced during any phase of the software development life cycle.

Answer: True

4. Question: A password is an example of something you are in the authentication process.

Answer: False

5. Question: Biometric authentication is considered convenient because it does not require the user to remember or carry anything.

Answer: True