Cybersecurity

Architecture and Design

2.1.2 Data Sovereignty and Protection

What is data sovereignty and protection?

Overview
The student will explain the importance of security concepts in an enterprise environment.

Grade Level(s)
10, 11, 12

Cyber Connections

- **Threats & Vulnerabilities**
- **Networks & Internet**
- **Hardware & Software**

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Teacher Notes:

CompTIA SY0-601 Security+ Objectives

Objective 2.1

- Explain the importance of security concepts in an enterprise environment.
    - Data sovereignty
    - Data protection
        - Data loss prevention (DLP)
        - Masking
        - Encryption
        - At rest
        - In transit/motion
        - In processing
        - Tokenization
        - Rights management

Data Sovereignty and Protection

Data Sovereignty

Data sovereignty is the concept that information that has been converted and stored in binary digital form is subject to the laws of the country in which it is located. There may be compliance regulations prohibiting the transfer of data into or out of the country in question. The idea of data sovereignty is very closely connected with cloud storage. As data is viewed and stored in different locations, it becomes very important to follow the proper laws.

Data Loss Prevention

Data loss prevention (DLP) is a strategy to keep private or proprietary data such as health data, personally identifiable information (PII), financial statements, proprietary diagrams, and other private information from being shared through unauthorized access. This means preventing users who should not have access to data from gaining access. We will look further into different types of DLP in later objectives.

Phantom of the Obfuscation

By definition, ***obfuscate*** means to make unclear or to confuse, bewilder, or stupefy. In cryptography, obfuscation is just a process of making something unclear. Obfuscation is not encryption; it is similar to having a sliding puzzle

Teacher Notes:

where all the pieces are there, just arranged in the incorrect order. With enough time and patience, you can put it together in a way that makes sense. The terms data ***masking*** and data obfuscation are used interchangeably.

Cryptography 101

Without going into too much detail, the term ***cryptography*** is used frequently in the world of cybersecurity. The two root words used to form cryptography come from the Greek words ***kryptós***, meaning "a secret" or "to hide", and ***graphein***, meaning "to study". Put together, cryptography is defined as the practice and study of writing or solving codes. In order to hide data, a cipher or key (algorithm) is used to ***encrypt*** (convert) and ***decrypt*** (convert back) a message. Starting with the ***plaintext***, the message to be sent which has not been encrypted yet, the cipher encrypts to ***ciphertext***, the message that has been encrypted that typically looks like a jumbled mess, and then the cipher decrypts back to plaintext. This process is known as ***encryption***.

States of Data

To prevent data loss, the state of the data must be considered. There are three states of data. Data is considered to be in use, in motion, or at rest. ***Data in use*** is data being used to execute some task. This could be a document being edited, an audio file being listened to, or an email being composed. Data in use is just what the name implies: data being used to inform the user, make decisions, or presenting information with others in some capacity. Protecting data in use includes preventing data leakage. This could mean preventing shoulder surfing, blocking malware on the machine, thwarting keyloggers that capture keystrokes, or preventing spyware from taking screenshots of open documents.

Data in motion is data being sent over a network or to a secondary storage device. Data sent over a network is where data can be at its most vulnerable and where it is more likely to encounter malicious users seeking to gain access to the data. Data in motion can also be data stored on removable media and physically ***in motion***. This could be a truck full of backup media, like tapes, in transit to an off-site, secure facility for warehousing. Protecting data in motion means encrypting data as it moves from one location to another in a network.

Data at rest is data that is stored in memory or on a disk drive. This data

Teacher Notes:

is sitting idle and stored for later use. Access to this data can either be authorized or unauthorized and should be monitored to see who accesses it and when. Protecting data at rest also means encrypting data as it is stored in memory or on disk.

Data in Processing

Data in processing refers to data that is collected and translated into usable information. Anyone is capable of doing this; however, it is recommended that a data scientist (or team) process the information so the output is not negatively affected. Data in processing goes through six steps: collection, preparation, input, processing, output, and storage.

Tokenization

Tokenization is the process of turning "sensitive" data into "non-sensitive" data, referred to as ***tokens***. Tokenization is useful in securing sensitive data because it replaces the original data with an unrelated value of the same length and format. Tokenized data differs from encrypted data because it cannot be deciphered or reversed.

Rights Management

Rights management refers to most forms of information control. Some examples include document rights management, information rights management (IRM), enterprise rights management (ERM), and digital rights management (DRM). Typically, IRM and ERM refer to protecting and controlling information within an Enterprise, whereas DRM and document rights management refer to shared documents security or licensing and control of paid content. Both the owner/creator of the content and the user of the content will have rights to consider.