2-2 Journal: Cybersecurity Fundamentals

Joshua Merren

Southern New Hampshire University

CYB-250-11621-M01 Cyber Defense

Professor Tchinda Mbuna

8 July 2024

Cryptography is a vital tool in cybersecurity that helps protect information by turning readable data into a coded form that only people with the correct key can read. This method is essential for keeping data safe when it is being sent across networks (data in motion) and stored on computers or other devices (data at rest). For data in motion, using encryption means that even if someone intercepts the data, they cannot understand it without the decryption key. Everyday internet use demonstrates this, as encryption protocols like SSL and TLS protect our online activities. These protocols keep our web browsing, email exchanges, and online shopping secure from outsiders who might want to steal our information. When physical security measures fail or a system is hacked, cryptography is critical in securing data at rest. Encrypting files and databases ensures that sensitive information remains unreadable to unauthorized users, which is crucial for protecting personal and business information. For example, when laptops, smartphones, or external drives are lost or stolen, the data stays protected if encrypted, thus preventing potential misuse of the information.

Threat modeling is a process used in cybersecurity to help identify and handle potential threats before they become a problem. It helps organizations understand what data needs to be protected, identify their systems' weaknesses, and determine the possible damage from different types of attacks. By analyzing potential threats, companies can decide where to use encryption more effectively to safeguard their data. For instance, if a threat model shows that specific business data can be accessed online, the company might encrypt this data to prevent unauthorized access. This proactive approach helps set up defenses against attacks that could lead to data breaches or leaks. This technique also allows organizations to prioritize security by focusing on the most significant risks. For example, suppose threat modeling identifies an internal database as vulnerable to attacks from the web. In that case, the organization can encrypt the data stored in the database to reduce the risk. The combination of threat modeling and cryptography helps protect critical information and builds a robust defense system that reduces the overall cyber-attack risk. This integrated approach is essential in creating a secure environment where the organization's and customers' data are well protected.