Topic 2 Discussion 1

Relate access control in the computer world to the physical world. In your own words, provide an example of physical access control and tie it back to the digital landscape. Often in cybersecurity, we use compensating controls to mitigate vulnerabilities. Identify some physical vulnerabilities related to your example. What are some compensating controls that could be used? Explain your reasoning.

Hello Class,

In the computer world, access control refers to the process of regulating who can access certain resources or information within a system. This concept can be related to physical access control in the real world, where mechanisms are put in place to restrict entry to specific areas or assets.

Physical Access Control:

Physical Access Control - A company uses keycard access to secure its office building. Employees are issued keycards that grant them entry to the building during working hours.

In the digital realm, access control can be likened to user authentication mechanisms such as passwords, biometrics, or security tokens that restrict access to sensitive data or systems. Just as keycards grant physical access to a building, proper authentication methods in the digital world allow authorized users to access protected information.

Physical Vulnerabilities:

Tailgating - Unauthorized individuals following an authorized person into a secure area.

Lost or Stolen Keycards - Keycards can be misplaced or stolen, potentially granting unauthorized access.

Compensating Controls:

Video Surveillance - Monitoring entry points to detect and deter unauthorized access through tailgating.

Two-Factor Authentication (2FA) - Implementing 2FA for digital systems to add an additional layer of security beyond passwords.

Access Logs - Tracking keycard usage and access attempts to identify anomalies and potential security breaches.

Reasoning:

Video Surveillance - By monitoring entry points, organizations can detect instances of tailgating and take immediate action to prevent unauthorized access.

Two-Factor Authentication (2FA) - 2FA strengthens digital access control by requiring users to provide two forms of identification, reducing the risk posed by lost or stolen passwords.

Access Logs - Keeping detailed access logs allows organizations to review keycard usage patterns, identify suspicious activities, and investigate security incidents effectively.

In both physical and digital contexts, implementing compensating controls is crucial to mitigating vulnerabilities and enhancing overall security posture. By recognizing potential weaknesses, organizations can deploy additional measures to bolster access control and protect their assets from unauthorized access or breaches.