Nama : Sasmita Rachmawati

Absen : 15

Lab - Security Controls Implementation

Objectives

- **Analyze security needs of an organization.**
- **Recommend security controls based on organizational needs.**

Background / Scenario

In this lab, you will recommend security controls based on the needs of the Greenville Public School system.

The school system consists of one high school, one middle school, and three elementary schools. The district serves about 2500 students, has a staff of 210 teachers, 220 administrators and support staff, and 25 maintenance staff. The internet point of presence and data center is housed in the high school, which also houses the administrative offices. The schools are interconnected to the high school over a redundant fiber optic network. The data center houses all of the required servers in one location.

Your company has been hired to analyze the physical security and cybersecurity of the Greenville school system. An incident recently occurred in which a high school student obtained a teacher's credentials and logged into the administrative network. The student altered his grades, deactivated CCTV cameras, and obtained phone numbers for students.

The director of security for the district recently left her job and the position had not been filled. Security had been implemented by a number of consultants and employees and had not been well documented. Your tasks is to propose security controls that should be implemented and analyze the current system to see if it utilizes those controls. The superintendent and school board have compiled the following list of security concerns. You will use as a starting point for your analysis:

- A wide range of computers, with aging hardware and software, are located haphazardly throughout the district, many in classrooms and learning labs.
- Some school districts nationally have faced lawsuits due to loss of parental information because of data breaches.
- Another school district in the state had to shut down until systems were restored after a ransomware attack encrypted data held on a number of computers in the district network.
- Academic records have been accessed and altered by students.
- A parent who was not authorized to see his child gained access to an after-school activity on school grounds that the child attended.
- The library server in the data center had been unplugged by cleaning staff in the past.

- Student information was disclosed by an administrative employee in response to a malicious email.

Required Resources

- Device with internet access

Instructions

Part 1: Review security controls

Review the definitions of the security control types and functions below.

Security controls can be divided into three types:

1. **Physical security controls** - implemented to control physical access to people, equipment, facilities, and information.

2. **Technical security controls** - implemented to protect hardware and software systems and the information that these systems transmit, process, or store.

3. **Administrative security controls** - are policies, procedures, rules, and guidelines that are followed by personnel in order to achieve the security goals of an organization.

Security controls are viewed as having three functions:

1. **Preventive** - stop security threats from occurring

2. **Detective** - identify unauthorized activity

3. **Corrective** - address unwanted activity by restoring systems to normal CIA status

Part 2: Complete a security controls grid

You will now complete the grid by recommending specific measures for each of the empty boxes in the grid. You will recommend both general security and cybersecurity measures, systems, or activities. Assume that the school district has no security in place at the present time.

Record your answers in the table below:

	Preventive	**Detective**	**Corrective**
Physical Controls	**Locked access to school buildings; restricted access to data centers; regular equipment maintenance; outdoor lighting**	**CCTV monitoring; door, window, and motion sensors; periodic vulnerability assessments**	**Rapid repair and replacement of critical equipment; reissue lost access cards; temporary facility rentals if needed**
Technical Controls	**Network and host-based firewalls; antivirus software;**	**Log monitoring; IDS/IPS systems; SIEM; network**	**Malware removal; restore data from**

	Preventive	Detective	Corrective
	multifactor authentication for sensitive data; VPN for remote access; system hardening; encryption of student data	**baselining and trend analysis**	**backups; patch management**
Administrative Controls	**Badging and registration of all visitors; security policies (passwords, access control); security awareness training; audit logs for student grades and access**	**Review access logs; asset tracking; user activity audits**	**Incident response planning and training; forensic analysis; post-incident user training**

Reflection Questions

1. Why are preventive physical controls important in schools?

Answer:

Preventive physical controls in schools are essential to protect students, staff, and resources. They ensure unauthorized individuals do not access sensitive areas or equipment, which helps prevent physical theft, damage, or tampering with critical systems, such as the data center or school facilities.

2. What preventive administrative controls are most effective against social engineering, including vectors that spread ransomware?

Answer:

The most effective administrative control is comprehensive user training. Educating staff and students on recognizing phishing attempts and social engineering tactics reduces the likelihood of attacks. Policies on password management and regular training reinforce good practices that prevent social engineering exploitation.

3. What is essential to preventing lasting damage from ransomware attacks while saving money on ransomware payments for restoration of data?

Answer:

A reliable data backup program is crucial. Regularly backing up data, especially storing backups offsite or on the cloud, ensures data can be restored without paying ransoms. Encouraging staff to save files on network drives instead of local storage further minimizes data loss in case of ransomware incidents.