Rossi Dea Agatha
SIB 4C – 2141762112

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	- Akses terbatas dengan kart uke Gedung sekolah - Akses admin terbatas untuk fasilitas jaringan dan pusat data - System pemadam kebakaran dan alarm kebakaran - Penerangan luar ruangan	- CCTV untuk memonitor aktivitas di sekitar dan didalam Gedung - Alarm pintu, jendela, dan sensor di area penting - Detector asap dan kebakaran	- Perbaikan segera atas kerusakan pada perangkat fisik - Penggantian kartu akses atau lencana yang hilang - Inventarisasi suku cadang untuk perangkat keras - Penyewaan fasilitas sementara jika ada kerusakan yang parah pada gedung
Technical Controls	- Firewall jaringan atau system pencegahan intrusi (IPS) - Firewall berbasis host dan antivirus - Autentikasi multifactor untuk akses ke data sensitive - Control aplikasi jaringan - Enkripsi data catatan siswa	- Monitoring akses log, analisis log host - Pemantauan keamanan jaringan, misalnya Sistem Deteksi Intrusi (IDS) - Penggunaan honeypot untuk mendeteksi potensi serangan	- Pengahapusan dan pencegahan malware - Pemulihan data dan gambar dari backup - Manajemen patch untuk system yang terdampak

Administrative Controls	- Pembuatan lencana bagi karyawan dan registrasi tamu - Pelatihan kesadaran bagi seluruh staf dan siswa - Penerapan kebiajakan kata sandi yang kuat dan regular - Kebijakan pengendalian akses berdasarkan peran	- Audit data sevara berkala, misalnya audit nilai siswa - Pengecekan dan review log AAA (Authentication, Authorization, Accounting) secara rutin	- Analisis forensic pada perangkat yang terindikasi terkena insiden - Latihan repons insiden dan perencanaan kontinuitas operasional - Pelatihan pasca insiden kepada pengguna terkait keamanan dan rekayasa sosial

Reflection Questions

1. Why are preventive physical controls important in schools?
    - Kontrol fisik preventif penting di sekolah untuk melindungi siswa dari potensi bahaya fisik, seperti akses orang yang tidak berwenang ke area sekolah. Selain itu, kontrol fisik juga melindungi peralatan jaringan dan komputer dari potensi kerusakan atau pencurian, menjaga keamanan data dan sistem yang tersimpan di pusat data.

2. What preventive administrative controls are most effective against social engineering, including vectors that spread ransomware?
    - Pelatihan keamanan bagi pengguna adalah kontrol administratif preventif paling penting untuk mencegah serangan rekayasa sosial dan ransomware. Melalui pelatihan ini, staf dan siswa dapat lebih waspada terhadap potensi phishing, email berbahaya, atau rekayasa sosial yang bertujuan mendapatkan akses tidak sah ke data sensitif.

3. What is essential to preventing lasting damage from ransomware attacks while saving money on ransomware payments for restoration of data?
    - Program backup data yang andal sangat penting untuk mencegah kerusakan berkepanjangan akibat serangan ransomware. Backup yang baik memungkinkan pemulihan data tanpa harus membayar tebusan. Selain itu, memastikan staf menyimpan pekerjaan mereka di server jaringan, bukan secara lokal, juga mengurangi risiko kehilangan data akibat serangan tersebut.