Access Control Categories

Module 4: Identity and Access Control

Access Control Categories

The access controls can be classified into three layers or categories, each category having different access control mechanisms that can be carried out manually or automatically.

- Administrative Controls
- Physical Controls
- Technical or Logical Controls

Administrative Control Components

Policy and Procedures

- A security policy is a high-level plan that states management's intent pertaining to **how security should be practiced** within an organization, **what actions are acceptable,** and **what level of risk** the company is willing to accept. This policy is derived from the **laws, regulations, and business objectives** that shape and restrict the company.
- The security policy provides direction for each employee and department regarding how security should be implemented and followed for noncompliance.
- Procedures, guidelines, and standards provide the details that support and enforce the company's security policy.

Personnel Controls

Personnel controls indicate how employees are expected to interact with security mechanisms, and address non-compliance issues pertaining to these expectations.

Change of Status: These controls indicate what security actions should be taken when an employee is hired, terminated, suspended, moved into another department, or promoted.

Separation of duties: The separation of duties should be enforced so that no one individual can carry out a critical task alone that could prove to be detrimental to the company.

Separation of duties

Example: A bank teller who has to get supervisory approval to cash checks over $2000 is an example of a separation of duties. For a security breach to occur, it would require collusion, which means that more than one person would need to commit fraud, and their efforts would need to be concerted. The use of separation of duties drastically reduces the probability of security breaches and fraud.

Rotation of duties means that people rotate jobs so that they know how to fulfill the obligations of more than one position. Another benefit of rotation of duties is that if an individual attempts to commit fraud within his position, detection is more likely to happen if there is another employee who knows what tasks should be performed in that position and how they should be performed.

Supervisory Structure and Security-Awareness Training

Supervisory Structure: Management must construct a supervisory structure that enforces management members to be responsible for employees and take a vested interest in their activities. If an employee is caught hacking into a server that holds customer credit card information, that employee and her supervisor will face the consequences?

Security-Awareness Training

This control helps users/employees understand how to properly access resources, why access controls are in place, and the ramification for not using the access controls properly.

Testing

This control states that all security controls, mechanisms, and procedures are tested on a periodic basis to ensure that they properly support the security policy, goals, and objectives set for them.

The testing can be a drill to test reactions to a physical attack or disruption of the network, a penetration test of the firewalls and perimeter network to uncover vulnerabilities, a query to employees to gauge their knowledge, or a review of the procedures and standards to make sure they still align with business or technology changes that have been implemented.

Physical

Physical controls support and work with administrative and technical (logical) controls to supply the right degree of access control.

Physical Control Components:

1) Network Segregation

Network segregation can be carried out through physical and logical means. A section of the network may contain web servers, routers, and switches, and yet another network portion may have employee workstations.

Each area would have the necessary physical controls to ensure that only the permitted individuals have access into and out of those sections.

Perimeter Security

The implementation of perimeter security depends upon the company and the security requirements of that environment.

One environment may require employees to be authorized by a security guard by showing a security badge that contains picture identification before being allowed to enter a section. Another environment may require no authentication process and let anyone and everyone into different sections.

Perimeter security can also encompass closed-circuit TVs that scan the parking lots and waiting areas, fences surrounding a building, lighting of walkways and parking areas, motion detectors, sensors, alarms, and the location and visual appearance of a building. These are examples of perimeter security mechanisms that provide physical access control by providing protection for individuals, facilities, and the components within facilities.

Computer Controls, Work Area Separation and Data backups

Computer Controls

Each computer can have physical controls installed and configured, such as locks on the cover so that the internal parts cannot be stolen, the removal of the floppy and CD-ROM drives to prevent copying of confidential information, or implementation of a protection device that reduces the electrical emissions to thwart attempts to gather information through airwaves.

Work Area Separation

Some environments might dictate that only particular individuals can access certain areas of the facility.

Data Backups

Backing up data is a physical control to ensure that information can still be accessed after an emergency or a disruption of the network or a system.

Examples of Physical Control

Fences

Locks

Badge system

Security guard

Biometric system

Mantrap doors

Lighting

Motion detectors

Closed-circuit TVs

Alarms

Backups

safe storage area of backups

Technical

Technical controls called logical controls are the s/w tools used to restrict the subject's access to objects. They can be core OS components, add-on security packages, applications, n/w h/w devices, protocols, encryption mechanisms, and access control metrics.

They protect the integrity and availability of resources by limiting the number of subjects that can access them and protect the confidentiality of resources by preventing disclosure to unauthorized subjects.

Technical Control Components

System Access

In this type, control of access to resources is based on the sensitivity of data, clearance level of users, and user's rights and permissions. As technical control for system access can be a user name password, Kerberos implementation, biometrics, PKI, RADIUS, TACACS, or authentication using smart cards.

Network Access

This control defines the access control mechanism to access different network resources like routers, switches, firewalls, bridges, etc.

Encryption and protocols and Auditing and Network Architecture

Encryption and protocols

These controls are used to protect information as it passes throughout an n/w and resides on computers. They preserve the confidentiality and integrity of data and enforce specific paths for communication to take place.

Auditing

These controls track activity within a n/w, on a n/w device, or on a specific computer . They help to point out the weaknesses of other technical controls and make the necessary changes.

Network Architecture

This control defines the logical and physical layout of the network, and also the access control mechanisms between different n/w segments.

Examples of Technical Controls

ACLs

Routers

Encryption

Audit logs

IDS

Antivirus software

Firewalls

Smart cards

Dial-up call-back systems

Alarms and alerts

Examples of Administrative Controls

- Security policy
- Monitoring and supervising
- Separation of duties
- Job rotation
- Information classification
- Personnel procedures
- Investigations
- Testing
- Security-awareness and training