Access Control Measures Implementation Report

Scenario

A company, SecureTech, operates a medium-sized IT infrastructure that includes an internal file server, a web application server, and a database server. The company wants to ensure that only authorized personnel can access specific resources based on their roles and responsibilities. The IT department has been tasked to implement access control measures to secure these resources.

Key Requirements:

1. Implement an Access Control List (ACL) to restrict access to specific servers.
2. Use an access control model to enforce policies for sensitive data.
3. Define user access levels to ensure role-based access.

Implementation

1. Access Control List (ACL)

An ACL has been implemented on the company's firewall to restrict access to the database server. The rules specify which IP addresses and user accounts are permitted to access the server.

ACL Configuration Example:

Rule	Source IP	Destination IP	Protocol	Port	Action
1	192.168.1.10	192.168.2.50	TCP	3306	Allow
2	192.168.1.0/24	192.168.2.50	TCP	3306	Deny
3	Any	192.168.2.50	Any	Any	Deny

- **Explanation:**
    - Rule 1: Grants access to the database server (192.168.2.50) on port 3306 for the IT administrator's IP address (192.168.1.10).
    - Rule 2: Denies access to the entire subnet (192.168.1.0/24) except for the specific IP allowed in Rule 1.
    - Rule 3: Denies all other access by default.

2. Access Control Model: Discretionary Access Control (DAC)

The company chose DAC to manage permissions for files and folders on the internal file server. DAC allows data owners to set permissions for their resources.

Example Implementation:

A project folder `/projects/marketing/` contains sensitive files. Permissions are configured as follows:

User/Group	Permission Level
marketing_manager	Read, Write
marketing_team	Read
it_admin	Full Control
other_users	None

- **Explanation:**
    - The marketing manager has read/write permissions to modify content.
    - The marketing team can only read the files.
    - IT administrators have full control for maintenance purposes.
    - All other users are denied access.

3. User Access Levels

SecureTech implemented three access levels for users:

1. **Administrator**:
    - Full access to all servers and resources.
    - Capable of modifying ACLs and managing user permissions.
2. **Manager**:
    - Access to departmental resources and applications.

    - Limited ability to share or modify files within their department.
3. **Employee**:
    - Restricted access to specific files and applications needed for their role.
    - No permissions to modify system configurations.

Example Policy:

- A marketing employee has access to `/projects/marketing/` with read-only permissions.
- A manager in marketing has both read and write permissions for the same folder.
- An IT administrator has full access to all system resources.

Conclusion

By implementing the above access control measures, SecureTech has enhanced its security posture, ensuring:

1. Only authorized users can access specific servers and resources.
2. Role-based permissions align with organizational policies.
3. Critical systems are protected from unauthorized access through strict ACLs and DAC policies.

Regular audits and updates to access controls will ensure continued security as the organization evolves.