Secure Authorization Models

4.3 Given a Scenario, Implement Identity and Access Management

Description

- In this episode, we will cover common authorization models including Role-Based Access Control(RBAC), Group-Based Access Control(GBAC), and Discretionary Access Control(DAC).

Resources

- N/A

Learning Objectives

- Define Role-Based Access Control(RBAC)
- Define Group-Based Access Control(GBAC)
- Define Discretionary Access Control(DAC)

Notes

- Authorization models
    - Role-based access control
        - Roles are created based on job function
            - DB Admin
            - DB Entry
            - DB Backup
        - Permissions are assigned to the roles
            - Permissions are typically fairly granular
            - Can be used to create specific permissions for individual roles in a team
        - Users are assigned to 1 or more roles
            - Users inherit permissions of the roles they are assigned to
    - Group-based access control
        - Groups are created based on department or other commonality
            - HR
            - IT
            - Dev
            - Finance
        - Permissions are set similiarly to that of RBAC
            - A bit braoder in scope
            - Tends to focus on the needs of the overall group
              Not of individual roles in said group
    - Discretionary
        - Data owner sets access/read/write/execute permissions at their discretion