

Introduction to Identity and Access Management

Mastering Identity and Access Management for Enhanced Security.

DEFINITION

Identity and Access Management (IAM) ensures that the right individuals access the right resources at the right times for the right reasons. It involves managing user identities and their access privileges within an organization.

KEY CONCEPTS

Authentication

The process of verifying a user's identity, often through passwords or biometrics.

Authorization

Determining what an authenticated user is allowed to do, such as accessing specific data.

User Provisioning

The creation, management, and deletion of user accounts and their access rights.

Single Sign-On (SSO)

A user authentication process that allows a user to access multiple applications with one set of login credentials.

Multi-Factor Authentication (MFA)

A security system that requires more than one form of verification to grant access.

EXAMPLES

- Using a fingerprint scanner to log into a secure system.
- Granting a new employee access to specific software tools after their account is created.
- Logging in once to access email, cloud storage, and project management tools.

MEMORY TIPS

- ★ Remember 'AAA' for Authentication, Authorization, and Accounting.
- ★ Use 'MFA' as 'More Factors Always' for Multi-Factor Authentication.
- ★ Think of SSO as 'Single Key for Many Doors' for Single Sign-On.

COMMON MISTAKES

- ✗ Confusing authentication with authorization.
- ✗ Neglecting to revoke access when employees leave.
- ✗ Using weak passwords despite security policies.

QUICK RECAP

Identity and Access Management is crucial for protecting organizational resources. It involves authentication, authorization, and user provisioning to ensure secure access. Remember the importance of MFA and SSO in enhancing security.