Identity and Access Management (IAM)

Introduction

IAM Introduction

- “Identity and access management (IAM) is the security discipline that enable the right individuals to access the right resources at the right times for the right reasons.” - Gartner

- IAM is a set of software tools and technologies including protocols that us designed to take care of the identity and access management for any organization.

IAM Introduction

- Tools of IAM are typically used by IT administrators to easily control users and digital assets of any organizations so that the workflow of the organization is efficiently managed.

- Users can include employee, partners, vendors customers etc..
  - The users could be humans, devices like (IOT) or software etc.
  - Thus IAM identifies these users and allocate right resources.

IAM in organizations

- Employees need to access their organization's resources like apps, files, data, computing resources etc.

- The traditional way of doing things was to have the vast majority of workers work on-site, where company resources were kept behind a firewall.
  - Once on-site and logged in, employees could access the things they needed.

- Now, however, hybrid work is more common and employees need secure access to company resources whether they're working on-site or remotely. **This is where identity and access management (IAM) comes in.**

IAM in organizations

- The organization's IT department needs a way to control what users can and can't access so that sensitive data and functions are restricted to only the people and things that need to work with them.

- Goal: IAM systems goal is to make sure that authentication and authorization happen correctly and securely at every access attempt.

Importance of IAM in cyber Security

- IAM (Identity and Access Management) plays a critical role in cyber security by ensuring that only authorized individuals have access to resources and data within an organization's network.

- **1. Controlled Access**: IAM allows organizations to control who can access specific resources, systems, and data.
  - It ensures that only authorized personnel can perform certain actions, **reducing the risk of unauthorized access and data breaches.**

Importance of IAM in cyber Security

- **2.Data Protection**: By implementing IAM, organizations can enforce granular access controls to sensitive data.
  - This prevents unauthorized users from viewing, modifying, or deleting critical information, reducing the risk of data leaks and data theft.

- **3. User Accountability**: IAM solutions provide accountability by enabling organizations to track and monitor user activities.
  - In case of a security incident, it becomes easier to identify the source of the breach and take appropriate measures.

Importance of IAM in cyber Security

- **4. Least Privilege Principle**: IAM adheres to the principle of least privilege, which means users are only granted the minimum level of access necessary to perform their job duties.
  - This minimizes the impact of a potential security breach as compromised accounts have limited access.

- **5. User Lifecycle Management**: IAM solutions facilitate efficient user lifecycle management.
  - It automates processes such as onboarding, offboarding, and role changes, reducing the risk of errors and ensuring that access permissions are up-to-date.

Importance of IAM in cyber Security

- **6. Compliance and Regulations**: Many industry regulations and data protection laws require organizations to implement strong IAM practices.
  - Adhering to these requirements helps organizations avoid legal consequences and financial penalties resulting from non-compliance.

- **7. Mitigation of Insider Threats**: IAM solutions help mitigate insider threats by monitoring user activities and detecting unusual behavior patterns.
  - This aids in identifying potential malicious activities by employees or contractors.

Importance of IAM in cyber Security

- **8. Cloud Security**: As organizations adopt cloud services, IAM becomes even more crucial in managing access to cloud resources.
  - IAM provides the necessary security controls to protect cloud-based data and applications.

Major drivers of IAM

1. Risk reduction/ security Improvement
2. Regulatory Compliance
3. End user Experience
4. Operational Efficiency
5. Cost Containment

1. Risk Reduction/ Security Improvement

- Timely and thorough de-provisioning of access when user changes job-function or leaves organization
- Perform access reconciliation detect unauthorized access to approved access.
- Provide improved accountability for control over changes to systems and applications (PAM)
- Ability to enforce strong and consistent password policies
  - Password management
  - Password synchronization
  - Reduced sign-on for different apps etc..

2. Regulatory Compliance

- IAM solutions make it possible to verify and manage identities, detect suspicious activity, and report incidents, all of which are necessary for meeting compliance requirements such as
  - Know Your Customer,
  - transaction monitoring for Suspicious Activity Reporting,
  - the Red Flags Rule etc.

- There are also data protection standards like
  - General Data Protection Regulation (GDPR),
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Sarbanes-Oxley Act (SOX).
  - Financial Services Authority (FSA).

2.Regulatory Compliance (Contd..)

- Compliance is regulated and verified by acts and regulatory bodies (given in previous slide).
- **Non compliance is viewed extremely serious and can result in severe penalties.**

- Compliance is one of the main business driving factor for organization wishing to implement an IAM solution.

- Companies have to know and be able to prove
  - Which user have access to which system;
  - That access for each user is warranted and approved
  - How incorrect access is corrected.

3. End User Experience

- Reduce the number of enterprise credentials
- Reduce the number of time a user has to provide log in with credentials
- Empowers the end user to manage their identity and credentials without having to call for help desk representatives.
- Business user have better and more accurate understanding of their systems

4. Operational Efficiency

- Enables new workers to be productive more rapidly.
- Automated provisioning provides less chance of provisioning errors.
- Empower delegated administrators to respond to user request in timely manner
- Increased speed and efficiency with automated provisioning

5. Cost Containment

- Provides self service capabilities
- Decrease IT security and Management cost through automation of identity and access management.
- Lower application development cost by providing reusable IAM services.

CIA for Information Security

- Protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

- Confidentiality
- Integrity
  - Authenticity
  - Accuracy
  - Non-Repudiation
- Availability

CIA: Confidentiality

- Examples of Confidential data
  - PII (Personal Identifiable Information)
  - PHI(Personal Health Information)
  - IP(Intellectual Property)

- Controlling Confidentiality
  - Encryption
  - Separation of duty
  - Least privileges

CIA: Integrity

- Authenticity
  - Provide assurance that a message, transaction or other exchange of data is from the source that claims to be from.
- Accuracy
  - The stored data on the system is accurate, trusted and not modified by unauthorized person.
- Non-Repudiation
  - Assure that sender or recipients can prove that they sent or received the message and cannot deny that.

CIA: Availability

- Redundancy & Failover
  - System need to be available all the time and failing one component shouldn't have an impact on the system operation.
- Accessibility
  - End users need to be able to access the system and applications all the time without interruption.
- Disaster Recovery
  - In case of disaster, system need to be restored and recovered as quickly as possible.

Quiz

- Virus is a software or computer program that connect itself to another software or computer program to harm computer system and corrupt its data. Choose the most relevant security principle that virus is against?

  1-Confidentiality

  2-Integrity

  3-Availability

Components of IAM

1. **Identification:** This involves identifying users and entities within the system.
   - Each user is assigned a unique identifier, such as a username or email address, which serves as their digital identity.

2. **Authentication:** Authentication is the process of verifying the identity of a user or entity attempting to access a system.
   - It ensures that the user is who they claim to be. Common authentication methods include passwords, multi-factor authentication (MFA), biometrics, and hardware tokens.

Components of IAM

3. **Authorization:** After a user is authenticated, authorization determines what actions and resources they are permitted to access.
   - It involves setting up permissions and access rights based on the user's role, group, or other attributes.

4. **User Provisioning:** User provisioning is the process of creating, modifying, and disabling user accounts and access privileges.
   - It ensures that users have the appropriate access throughout their lifecycle within the organization.

Components of IAM

5. **Single Sign-On (SSO):** SSO enables users to log in once and gain access to multiple systems or applications without the need to re-enter credentials for each one separately.
   - It enhances user convenience while improving security.

6. **Role-Based Access Control (RBAC):** RBAC is a method of managing access based on a user's assigned role within the organization.
   - Instead of specifying permissions for each user individually, permissions are assigned to roles, and users are added or removed from those roles as needed.

Components of IAM

7. **Multi-Factor Authentication (MFA):** MFA adds an extra layer of security by requiring users to provide multiple forms of verification, such as a password, a fingerprint scan, and a one-time PIN sent to their mobile device, before gaining access.

8. **Identity Federation:** Identity federation allows users to access resources across multiple organizations or systems using the same set of credentials.
   - It establishes trust between different identity providers and service providers.

Components of IAM

9. **Access Logging and Auditing:** This component involves recording and monitoring user access activities for security and compliance purposes.
   - It helps track who accessed what resources and when.

10. **Privileged Access Management (PAM):** PAM focuses on securing and managing access for privileged users, such as system administrators, who have elevated access rights.
    - It enforces strict controls and monitoring over these accounts.

Components of IAM

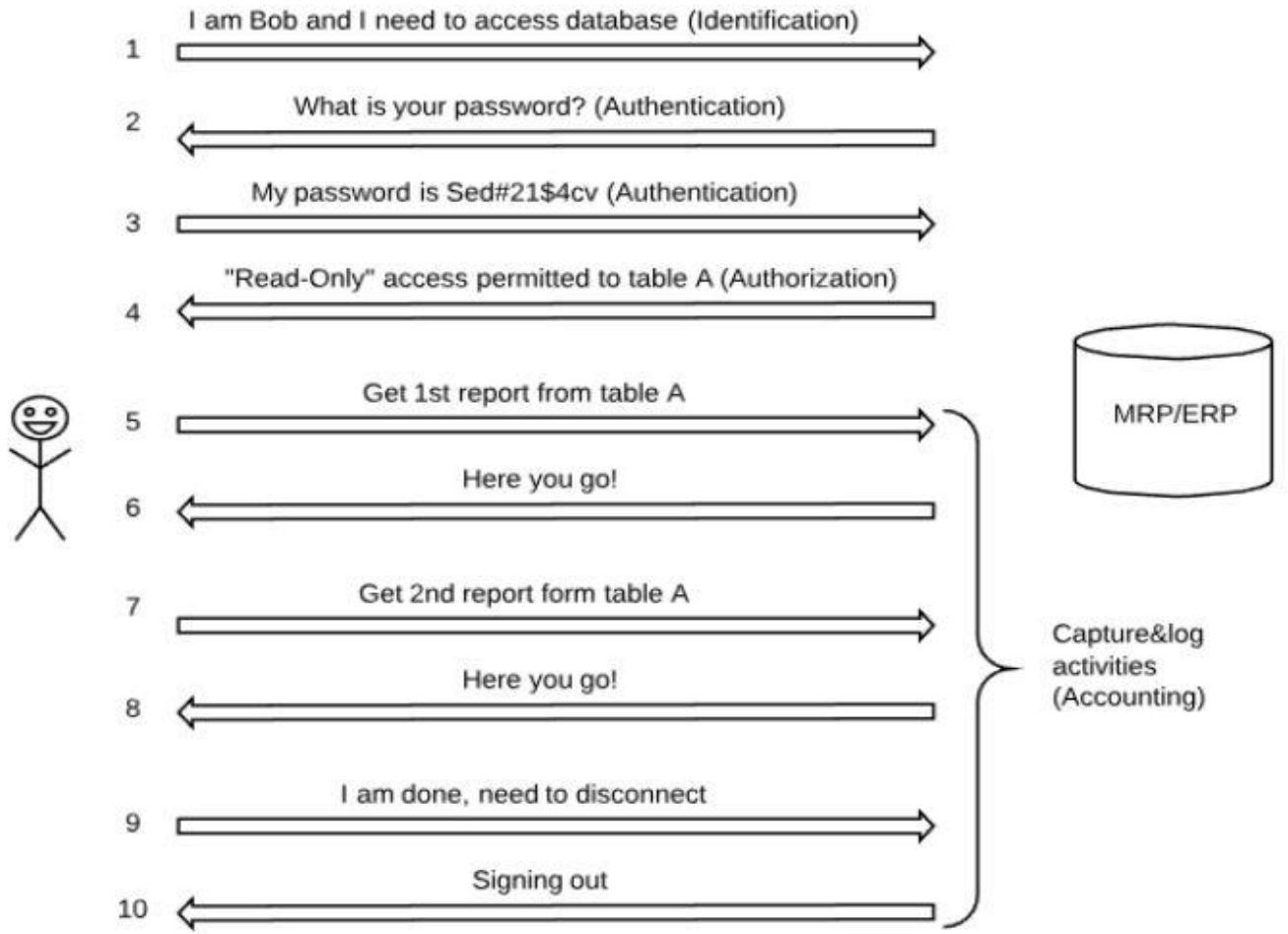
11. **Identity Management:** Also known as IDM, It is a framework that takes care of the identities of the users of enterprise.
    - It is a part of IT security for enterprise.
    - Uses AD, OpenLDAP or similar directories in the background for management of Identities.
12. **Password Management:** Associated with the user names.
    - It is subjected to password policies of the organizations.
    - System identifies a user, when right password is provided at the time of logging in.

IAAA

- Set of controls to govern accessing to digital resources and data and a mechanism to audit and track the usage for security and billing purposes.

- Identification
- Authentication
- Accounting
- Authorization

IAAA


I am Bob and I need to access database (Identification)
1
What is your password? (Authentication)
2
My password is Sed#21$4cv (Authentication)
3
"Read-Only" access permitted to table A (Authorization)
4
Get 1st report from table A
5
Here you go!
6
Get 2nd report form table A
7
Here you go!
8
I am done, need to disconnect
9
Signing out
10
MRP/ERP
Capture&log activities (Accounting)

Information Security Concepts

- **Separation of duty:** Segregation or separation of duty concept means to ensure critical roles are not assigned to single user to avoid any possibility of fraud or similar malicious activity.

- **Least privileges:** The “Least privilege” or “need to know ” concept means minimum information must be shared with subjects, and that information.

- **Job rotation:** When one person is on the same job for a long time, that would increase the risks of frauds and collusion. Job rotation is control to detect and prevent errors and frauds.