Identity Access Management (IAM) is an important and crucial aspect of cybersecurity that focuses on managing user access and permission to sensitive digital resources. IAM’s ensures that the designated persons, machines, and software components can access the right resources at a given time, for the intended purpose. The system design prevents the unauthorized access from intruders, while allowing authorized users access to perform their intended tasks.

IAM originated from the need to secure digital resources in an era where cyber threats are ever more prominent, and the overall complexity and sophistication has increased. Organizations started to incorporate more digital measures into their workflow such as web applications, databases, and cloud services. These resources thus needed to be managed to allow access to users based on importances and capabilities of utilizing the resources. Through this IAM’s became a pivotal pillar to address these challenges, providing a more structured and manageable approach to the management of user identities and access rights.

The landscape of Identity Access Management involves numerous components such as:

Identity Management

* This identifies and involves the management of the lifecycle of digital entities from user registration to account deprovisioning. This ensures that identities are created, updated and synchronized across numerous systems and platforms, maintaining consistency and security.

Authentication

* Through various authentication methods developed throughout the years, means of identifying users and devices ensuring that legitimate users are able to gain access to resources.

Authorization

* The procedure of granting access to a user with given permission/authority to resources. This ensures that users have access to the necessary resources for their job functions, enhancing security and efficiency.

Access Control

* The implementation of policies defining who can access resources and under what conditions. This is based on user roles, groups, attributes and contextual factors. This ensures appropriate access is granted in a manner that aligns with the organization’s security policies and compliance procedures.

Identity Federation

* Developed utilizing numerous protocols like Security Assertion Markup Language (SAML) and OAuth, IAM’s are able to establish trusted and secure relationships between systems. This allows for a seamless pathway for users to access resources across organization boundaries, using their existing credentials from other systems.

Provisioning and Deprovisioning

* IAM provides systematic functionalities for user creation and dismissal, ensuring efficient and accurate user account creation for resource access, along with prompt revocation of access when the user no longer requires the resources. This enhances security and compliance by ensuring access rights and management through the user lifecycle.

Monitoring and Reporting

* To ensure continuous compliance and assessment of security risks, IAM systems are able to generate reports on user action and activity. This is done via tracking or surveillance on user activity (timestamping and logging), flagging of suspicious behavior and maintaining of auding trails. These measures are essential for monitoring the security and usage patterns of the environment and allow for ambling response towards threats.

Security and Compliance

* Implementation of identity governance processes, such as access certification, role-based access control, and audit trails as mentioned in the monitoring and reporting aspect of IAM, ensures compliance with regular requirements, industrial standards, and internal policies. Aided with the implemented measures to prevent unauthorized access, enforces security measures.

These areas of the IAM landscape encompass a wide range of practices and technologies designed to manage the digital identities and control access to resources securely and efficiently. To address the complexity of managing digital identities and access right to resources and services, while also complying with security policies, ensuring that only authorized users have access, numerous technological landscape strategies were developed and implemented. Some of these landscape strategies are Single Sign-On (SSO), Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC).

Single Sign-On (SSO), a technology that allows for users to login once and gain access to multiple applications and services without needing additional authentication. Through this, user experience is simplified by reducing the need to remember numerous passwords and streamlining the login process. SSO can be implemented through various methods of the IAM landscape, one of which being federated identity. Users authenticate themselves through a central identity provider and gain access to multiple systems without the need for a separate log in to various systems each time. The means of SSO minimizes the risk of password related security breaches as a strong means of signing in reduces the environmental factor of multiple weak, reused or common passwords. The downside to this method is the overall complexity through the integration process, especially with legacy systems and dealing with different authentication protocols. If implemented properly SSO is an important landscape strategy for further improving IAM.

Security measures that require users to provide two or multiple verification factors to gain access to resources, are Multi-Factor Authentication (MFA). This method incorporates a regular password for user identification and multiple other user input to verify the authorized user. Password Utilization, Something personal to the user or a biometric reading act as layers for MFA. Tools such as google authenticator, RSA SecurID are some tools that can be implemented into the IAM system to provide a robust authentication mechanism. A drawback to MFA would be the significance of false positives, this is where legitimate users are locked out due to issues with the MFA process, but overall, with proper implementation and tool usage, the risks associated with password breaches are reduced, as it ensures that even if a password is compromised, unauthorized access is prevented.

Role-Based Access Control (RBAC) is a method of managing access to resources based on the role assigned to users within an organization. Instead of granting access to rights based on individual identities, RBAC assigns permission based on roles and responsibilities of users. This approach simplifies access management and reduces administrative overhead by ensuring users only have access to the given resources their role permits. This complies with policies and strengthens IAM access control, while improving monitoring and reporting mechanisms. IAM systems often include RBAC features that allow organizations to assign roles and privileges accordingly. RBAC upholds the concept of least privilege, minimizing the risk of data breaches and streamlines provisioning and deprovisioning of users. The downside to utilizing RBAC is the complexity of managing the roles and permissions within an organization and if implemented incorrectly, misconfiguration can occur. Thus proper record keeping of roles and permissions must be accounted for, along with proper handover procedures and implementation.

These technologies are integral to the IAM landscape, each playing a crucial role in enhancing security, streamlining user access and ensuring compliance with regulatory requirements and polices. SSO, MFA and RBAC implementation creates a secure and efficient IAM framework for organization of varying sizes.

Sources

<https://www.linkedin.com/pulse/identity-access-management-iam-paulo-monteiro-xckrf/>

<https://www.pendello.com/blog/identity-and-access-management-iam-security-best-practices>

<https://www.veritas.com/information-center/identity-and-access-management>

<https://www.silverfort.com/glossary/identity-and-access-management-iam/>

<https://www.microsoft.com/en-us/security/business/security-101/what-is-identity-access-management-iam>

<https://auth0.com/docs/get-started/identity-fundamentals/identity-and-access-management>

<https://highervista.medium.com/cybersecurity-identity-and-access-management-iam-and-role-based-access-control-rbac-bcf8c8d86b43>