Identity and Access Management (IAM) Best Practices

Identity and access management (IAM) refers to policies, procedures, and tools that govern the identification, authentication, and authorization functions of networking, both at and inside the network edge. This framework enables the right entities (users or things) to access the required resources (applications or data) while restricting unauthorized access to the rest of the network.

It allows IT admins to assign a single identity to each entity, authenticate their login, authorize their role- and attribute-based access privileges, and monitor and manage the entire lifecycle of user identities, from creation to deletion. At its crux, IAM optimizes IT workload, enhances security, improves stakeholder engagement, and ensures a consistent user experience.

In this article, we learn about best access management practices and highlight common access management mistakes for IT managers to avoid.

5 access management best practices

An IAM technology is only as strong as the identity and access management policies and practices that support it. Its implementation requires proper planning for effective security yields. Let's learn the top 5 access management practices.

1. Implement multi-factor authentication

Passwords are vulnerable to hacking and unauthorized access. Their inadequacy for secure access to services or applications requires an additional layer of security. MFA is an authentication mechanism that requires users to provide two or more forms of evidence to authenticate their identity before getting access.

In addition to username and password, MFA mechanisms may require users to input one or more of the popular MFA methods, including one-time passwords (OTPs), biometric authentication, push notifications, smart cards, hardware tokens, etc. This way, MFA reduces the risks associated with stolen or weak passwords.

2. Enforce strong password policies

Strong password implementation is required by notable regulatory frameworks, such as GDPR and CCPA. A strong password requires uniqueness, strength (minimum 8 characters, combination of upper and lowercase, symbols, and numericals), and difficulty with guessing. Additionally, passwords should be regularly updated, and users should be encouraged not to use the same password across multiple accounts. Most importantly, even if used alongside MFA and SSO, the role of strong passwords can't be ignored.

3. Use single sign-on (SSO)

SSO reduces hassles with multiple usernames and passwords. It allows users to access multiple systems and applications across an organization with a single set of credentials. It improves the user experience, simplifies administration, enhances security, saves time, and adds to cost savings. It provides a centralized authentication system for easier user activity monitoring and real-time access control. It eases authentication and reduces the hassle of remembering multiple sets of usernames and passwords.

4. Use the principle of least privilege

The principle of least privilege involves restricting access to sensitive data, limiting administrative privileges, segregating duties, and implementing access controls. It governs users' maneuvering through the network, limiting their access to only those resources that their jobs or functions require. The goal of least privilege is to reduce the attack surface by limiting the potential damage that could be caused by an insider threat or a malicious user who has gained access to a user's account.

5. Create a single source of truth for all access and permissions

The concept of structuring information in such a way that it acts as a single definitive, trusted source for a specific data element is known as a single source of truth. It avoids inconsistencies and confusion caused by having multiple versions of the same information. This concept is achieved by creating a centralized repository that is the sole source of a particular piece of data for all applications, systems, or users. It helps organizations improve data quality, increase efficiency, and derive better decisions.

4 common access management mistakes to avoid

1. Forgotten user accounts

Forgotten user accounts may be used by attackers to gain unauthorized access to sensitive resources. These are accounts that stay active in the system even after their need for an

assigned role or task is officially terminated. To prevent risks with forgotten accounts, a system for regularly reviewing user accounts (automated or manual) to identify and disable inactive or forgotten accounts should be established.

2. Overprovisioning access privileges

Overprovisioning access privileges means granting more access rights to users than are actually required. For instance, privileges are assigned to users without considering their actual job roles and responsibilities. To avoid overprovisioning, organizations should follow the principle of least privilege, and roles and attribute-based access privileges should be reviewed on a regular basis.

3. Infrequent access reviews

Infrequent access reviews occur when user access to resources is not regularly reviewed. It involves reviewing and auditing user access to the system, data, and applications to ensure that access privileges are still necessary as per the users' job profiles and responsibilities. Access reviews ensure that issues like overprovisioning and forgotten accounts are under control.

4. Not having a system for who has access to what

Not having a system to track who has access to what increases the difficulty of knowing who has access to what resources, making it challenging to identify unauthorized access and potential security threats. To mitigate this issue, an access management system should be in place to track and manage access privileges across all systems, applications, and data.

Conclusion

Identity and access management guards an organization's valuable IT resources from both inside and outside threats. It enables organizations to manage compliance, user awareness, insider threats, and protection against penalties. With a unique identity and continuous monitoring of their movement through the network, IAM scans for potential security threats and records activities for troubleshooting and auditing purposes.