Identity and access management

Security is more than simply combining processes and technologies to protect assets. Instead, security is about ensuring that these processes and technologies are creating a secure environment that supports a defense strategy. A key to doing this is implementing two fundamental security principles that limit access to organizational resources:

- The **principle of least privilege** in which a user is only granted the minimum level of access and authorization required to complete a task or function.
- **Separation of duties**, which is the principle that users should not be given levels of authorization that would allow them to misuse a system.

Both principles typically support each other. For example, according to least privilege, a person who needs permission to approve purchases from the IT department shouldn't have the permission to approve purchases from every department. Likewise, according to separation of duties, the person who can approve purchases from the IT department should be different from the person who can input new purchases.

In other words, least privilege *limits the access* that an individual receives, while separation of duties *divides responsibilities* among multiple people to prevent any one person from having too much control.

Note: Separation of duties is sometimes referred to as segregation of duties.

Previously, you learned about the authentication, authorization, and accounting (AAA) framework. Many businesses used this model to implement these two security principles and manage user access. In this reading, you'll learn about the other major framework for managing user access, identity and access management (IAM). You will learn about the similarities between AAA and IAM and how they're commonly implemented.

Identity and access management (IAM)

As organizations become more reliant on technology, regulatory agencies have put more pressure on them to demonstrate that they're doing everything they can to prevent threats. **Identity and access management** (IAM) is a collection of processes and technologies that helps organizations manage digital identities in their environment. Both AAA and IAM systems are designed to authenticate users, determine their access privileges, and track their activities within a system.

Either model used by your organization is more than a single, clearly defined system. They each consist of a collection of security controls that ensure the *right user* is granted access to the *right resources* at the *right time* and for the *right reasons*. Each of those four factors is determined by your organization's policies and processes.

Note: A user can either be a person, a device, or software.

Authenticating users

To ensure the right user is attempting to access a resource requires some form of proof that the user is who they claim to be. In a video on authentication controls

, you learned that there are a few factors that can be used to authenticate a user:

- **Knowledge**, or something the user knows
- **Ownership**, or something the user possesses
- **Characteristic**, or something the user is

Authentication is mainly verified with login credentials. **Single sign-on** (SSO), a technology that combines several different logins into one, and **multi-factor authentication** (MFA), a security measure that requires a user to verify their identity in two or more ways to access a system or network, are other tools that organizations use to authenticate individuals and systems.

Pro tip: Another way to remember this authentication model is: something you know, something you have, and something you are.

User provisioning

Back-end systems need to be able to verify whether the information provided by a user is accurate. To accomplish this, users must be properly provisioned. **User provisioning** is the process of creating and maintaining a user's digital identity. For example, a college might create a new user account when a new instructor is hired. The new account will be configured to provide access to instructor-only resources while they are teaching. Security analysts are routinely involved with provisioning users and their access privileges.

Pro tip: Another role analysts have in IAM is to deprovision users. This is an important practice that removes a user's access rights when they should no longer have them.

Granting authorization

If the right user has been authenticated, the network should ensure the right resources are made available. There are three common frameworks that organizations use to handle this step of IAM:

- Mandatory access control (MAC)
- Discretionary access control (DAC)
- Role-based access control (RBAC)

A system administrator deciding to grant users and an operating system access to data.

Mandatory Access Control (MAC)

MAC is the strictest of the three frameworks. Authorization in this model is based on a strict need-to-know basis. Access to information must be granted manually by a central authority or system administrator. For example, MAC is commonly applied in law enforcement, military, and other government agencies where users must request access through a chain of command. MAC is also known as non-discretionary control because access isn’t given at the discretion of the data owner.

A data owner choosing to grant specific users access to their data.

Discretionary Access Control (DAC)

DAC is typically applied when a data owner decides appropriate levels of access. One example of DAC is when the owner of a Google Drive folder shares editor, viewer, or commentor access with someone else.

A system administrator assigning users to specific roles that have predefined access levels.

Role-Based Access Control (RBAC)

RBAC is used when authorization is determined by a user's role within an organization. For example, a user in the marketing department may have access to user analytics but not network administration.

Access control technologies

Users often experience authentication and authorization as a single, seamless experience. In large part, that’s due to access control technologies that are configured to work together. These tools offer the speed and automation needed by administrators to monitor and modify access rights. They also decrease errors and potential risks.

An organization's IT department sometimes develops and maintains customized access control technologies on their own. A typical IAM or AAA system consists of a user directory, a set of tools for managing data in that directory, an authorization system, and an auditing system. Some organizations create custom systems to tailor them to their security needs. However, building an

in-house solution comes at a steep cost of time and other resources.

Instead, many organizations opt to license third-party solutions that offer a suite of tools that enable them to quickly secure their information systems. Keep in mind, security is about more than combining a bunch of tools. It’s always important to configure these technologies so they can help to provide a secure environment.

Key takeaways

Controlling access requires a collection of systems and tools. IAM and AAA are common frameworks for implementing least privilege and separation of duties. As a security analyst, you might be responsible for user provisioning and collaborating with other IAM or AAA teams. Having familiarity with these models is valuable for helping organizations achieve their security objectives. They each ensure that the right user is granted access to the right resources at the right time and for the right reasons.

Resources for more information

The identity and access management industry is growing at a rapid pace. As with other domains in security, it’s important to stay informed.

- IDPro

© is a professional organization dedicated to sharing essential IAM industry knowledge.

Revision #1
Created 27 July 2023 17:02:17 by naruzkurai
Updated 15 August 2023 18:44:12 by naruzkurai