Security Advice: How to Bridge the Gap Between Authentication & Authorization

AN OPPORTUNITY TO EDUCATE BUSINESS LEADERS AND IT DECISION MAKERS

The second Tuesday in April marks “Identity Management Day.” Created by the Identity Defined Security Alliance (IDSA), this special occasion — which is having its inauguration in 2021 — is an opportunity to educate business leaders and IT decision makers on the importance of identity management and key related components, such as governance, best practices, processes, and technology.

While this awareness-raising has been important for many years — after all, hackers and digital identity thieves have been around for decades — it is more critical today than ever before. **Consider the following:**

- 74% of data breaches start with privileged credential abuse.
- 65% of companies have over 1,000 stale user accounts.
- «123456» was the most used password in 2020. It has been used by more than 2.5 million people and exposed more than 23 million times in data breaches.

However, while managing identities across a company is an essential practice, in theory, it is challenging in reality. To understand why, it is helpful to take a step back and look at two related but distinct functions: **identity management and access management.**

About Identity Management

Identity management is about combining digital elements and entries in a centralized database, in order to create a unique designation for each user. These designations are monitored, adjusted, and deleted as needed in order to enforce security, while providing users with the permissions necessary to carry out their tasks.

About Access Management

Access management governs whether or not users are entitled to access certain resources, apps, databases, areas of the network, and so on. It encompasses all policies, processes, methods, systems, and tools to maintain access that is privileged within a digital environment.

Authentication vs. Authorization

Obviously, there is overlap between identity management and access management, since they are both fundamentally designed to support a strong information security program, while still facilitating user productivity. This is why most members of the general public see them as synonymous. In fact, it is not uncommon to come across articles that treat them as essentially the same thing.

However, there is a crucial difference between identity management and access management: **the former is essentially about authentication (who a user is), while the latter is essentially about authorization (what an authenticated user can access).**

The Challenge of Enforcing Identity Management

One of the principles of identity management is establishing an authoritative source of trusted identity data (i.e., authentication attributes and subscriber attributes). But at the current time, technologies such as networking equipment, legacy systems, phones, and cameras cannot use a federated system. And while it is theoretically possible to manually create and maintain unique identity accounts for every user in an organization, in practice it is not feasible. To say that it would take a major effort is an understatement. It would be Herculean!

Some Shared Accounts Are Necessary

Complicating matters is the fact that in many organizations, certain activities must be performed using shared (i.e., privileged) accounts. Examples include:

- Domain Administrator Accounts
- Local Administrator Accounts
- Emergency Access Accounts
- Application Accounts
- System Accounts
- Domain Service Accounts

With shared accounts, identity is not exclusively associated with a specific user. Rather, it is associated with a role, team, or group.

And so, what is the most pragmatic and sustainable way for organizations to bridge the gap between identity management (authentication) and access management (authorization)? **The answer is to implement a Privileged Access Management (PAM) system.**

Why a PAM System Makes Sense

A PAM system uses role-based access control (RBAC) to function as a gatekeeper for shared accounts, adding a critical layer of privileged account monitoring and auditing through features such as:

- A secure vault that safely and properly stores credentials and other sensitive data that must be shared across multiple users (e.g. software license keys, etc.).
- Account discovery, which automatically scans and discovers privileged accounts from an Active Directory provider (more on this below).
- Account checkout request, which notifies Sysadmins and allows them to approve or reject the request on a case-by-case basis (and in the case of approvals, set a time limit for access to avoid privileged accounts being left unattended).
- Automated password reset upon check-in.

PAM and Account Discovery

Research has found that 88% of organizations with more than one million folders lack appropriate access limitations, and 58% of companies have more than 100,000 folders accessible to all employees. The Account Discovery aspect of a PAM system identifies these privileged accounts, so they can be updated, monitored, or deleted. Conversely, standalone identification providers, such as identity access management (IAM) systems, databases, network equipment, and servers, must be queried to discover accounts.

Privileged Session Management

In addition, more sophisticated PAM systems support Privileged Session Management (PSM). This utilizes a specialized server that brokers authentication behind-the-scenes, and can even record the activity of remote sessions. PSM is especially important for organizations that have contractors and “boomerang” employees (i.e., employees who leave the organization and then return). These users typically need more scrutiny and limited access.

Dual Accounts

Organizations are also advised to create dual accounts for higher privilege users. The first account has relatively limited access and is for day-to-day tasks. The second account has relatively more access and is for administrative duties. Obviously, this second account is managed by the PAM system and configured with enhanced security, such as account brokering and password rotation after use.

The Bottom Line

In an ideal world, organizations would use a single identity for everything. But in the real world, things are more complicated — and challenging! To stop hackers and rogue insiders, organizations need a pragmatic way to bridge the gap between authentication and authorization. And this is not just a top priority for large enterprises, as 43% of cyberattacks are carried out against SMBs, and the average cost for just a single breach has surpassed $200,000 — which is more than enough to put many smaller firms out of business within a matter of months.

A PAM system achieves the critical objective of protecting resources and accounts when user access cannot be federated. When a PAM system is integrated with an IAM and customized with alerts and an approval workflow, organizations establish a single pane of glass that generates total visibility across complex infrastructures. This is a major and frankly mandatory step towards protecting data, enforcing compliance, and enabling users to do their jobs.