WHO IS THIS?

THE IMPORTANCE OF IDENTITY AND ACCESS MANAGEMENT

Anyone who runs a modern business should take Identity and Access Management (IAM) seriously. Why? The surge in remote work, more interconnectivity across diverse platforms, and the crucial need to manage both human and machine identities are just three reasons that come to mind. But don't let the technical name scare you away. In this blog, I'll break down the who/what/why of IAM and I promise to keep it conversational. So, grab your favorite beverage, and before you can take your last sip, you'll have what you need to add IAM to your next sales conversation.

The Basics: Who Are You, Really?
Imagine you are at a fancy party (remember those?). You walk up to the entrance, and the bouncer gives you the once-over. What is their job? To verify your identity! They want to make sure you are on the guest list and not some party-crashing imposter.

Well, IAM is like that bouncer, but for the digital world. IAM answers the question, "Who is this?" And no, it is not an existential crisis; it is a framework of policies and technologies for managing who gets access to what in an organization's systems.

The Players: Meet the Cast

1. Users: These are the stars of our show—the people (or sometimes robots) who need access. Think employees, contractors, partners, clients, third-party vendors, and even that know-it-all AI assistant you chat with.

2. Identities: Identities are like backstage passes. They represent users and their roles. So, if you are an employee, your identity might grant you access to the company intranet, the coffee machine, and the swag storeroom (shhh!).

3. Access: This is the golden ticket! Access means getting into the VIP areas—the files, databases, apps, and servers. But not everyone gets the same access. Some folks get the red-carpet treatment into the secret speakeasy, while others hover near the break room.

The Challenges: Drama Behind the Scenes

1. Too Much Back-Stage Access
Larry from Accounting has access to the CEO's expense reports. Why? No one knows. It is like giving the janitor the keys to the executive washroom. IAM helps prevent such mishaps by ensuring that Larry only sees what he needs (sorry, Larry).

2. The Password Shimmy
Ah, passwords—the dance of frustration! IAM aims to simplify this. Single Sign- On (SSO) lets an individual waltz into multiple systems with one password. No more juggling a dozen post-it notes with cryptic codes!
3. The Turnover Tango

When employees leave, it is like a dramatic exit scene. IAM ensures their access gets revoked promptly. Otherwise, they might haunt an organization's servers forever (cue Friday the 13th music).

The Tools: IAM Superpowers

1**. Authentication:** The "Are you who you say you are?" check. Passwords, biometrics, or secret handshakes—it is all here.

2. Authorization: Deciding what you can access. Think of it as the velvet rope at the club. VIPs get in; crashers stay out.
3. Role-Based Access Control (RBAC): Assigning roles like "Sales Ninja" or "Database Wizard". Each role has specific powers. Like rolling a 20 in Dungeons and Dragons while creating your character…it's important to choose wisely!

4. Passwordless Credentials: The newest "hot" conversation, passwordless login capabilities through biometric scanning such as facial recognition, fingerprints, iris, or even voice is a way to quickly identify a user and control the breadth of access.

The Grand Finale: Why IAM Matters

1. Security: IAM locks the doors, bolts the windows, and sets up the “sharks with lasers” alarm. No unauthorized guests allowed!

2. Productivity: IAM streamlines access. No more waiting for IT to grant permissions.

3. Compliance: Auditors love IAM. It is like their favorite detective novel—full of logs, trails, and evidence.

So, my friends, think of IAM as the digital bouncer every organization should have in their corner. And think of Telarus when you need education and support to help connect you to the right IAM solutions for your customers.
Until next time, stay secure, stay curious, and keep those passwords strong!

By Jason Stein, VP of Cybersecurity, Telarus