CLOUDKNOX
BLOG

Blog Entry
November 30, 2018

Authentication vs. **Access Controls** vs. **Authorization**

Understanding the distinction between authentication and authorization has long been a prerequisite to any discussion of cybersecurity. The patterns emerge naturally from basic goals of security – denying undesired access to your infrastructure, applications, and data.

In the past, access control has largely been synonymous with authorization. However, the highly automated and dynamic nature of cloud infrastructure demands that we reexamine these concepts by deconstructing their true differences as follows:

Authentication

Authentication is the first step of the process. Its aim is simple – to make sure the identity is who they say they are. We run into it daily both in digital (username/password) and analog forms (ID/passport).

Access Control

Access control is the addition of extra authentication steps to further protect important segments. Once the identity proves they are who they say they are, access is granted. With access comes the authority to perform actions on whatever it is the identity has access to.

Authorization

Authorization defines the set of actions that the identity can perform after gaining access to a specific part of the infrastructure, protecting from threats that access controls alone are ineffective against.

An Analogy

Let's step away from definitions and jargon for a minute and explore the important distinctions through a 'case study.'

Imagine the common thriller plot we've all seen before:

- Government scientist create an ingenious device, with the potential to do immense good. (But also catastrophic evil – in the wrong hands)
- Some nefarious group learns of its existence and seeks to steal it.
- Of course the good guys have anticipated this, and have sought to protect the device by having it in a *secure room* on a *secure level* inside a *secure building*.

Let's imagine the steps our bad guys will have to go through

- They will have to swipe a key card from a guard to get into the building.
- To access the highest level, where the device is, they will have to find an administrator and use his fingerprint to get the elevator moving.
- Finally, they will need to coerce the key code from one of the scientists to access the room and steal/operate the device.

This scenario represents a typical security protocol involving authentication and access control tools. Each step involves our bad guys bypassing the authentication assigned to a role (guard, admin, scientist) and thereby gaining access to the highly sensitive spot where the device is located.

In movies the good guys always win. The amount of time and effort it takes to get access to each stage, through compromised credentials, gives the hero enough time to save the day.

However, lets consider some alternative plots:

A. A government scientist accidentally punches in the wrong codes and the device is destroyed.

B. Scientist Fred sabotages part of the project because he is jealous of the success of scientist Susan.

C. One of the scientists becomes sympathetic to the villainous cause and damages the device.

These scenarios make for short and terrible movie plots, but they are a realistic example of the type of threats organizations face to their critical infrastructure.

What is worse, access controls are powerless against these threats. The people in question had legitimate access to the device. And though their access was legitimate, they should not have had the authorization to perform sabotaging actions.

Here is a graphic for those of you who prefer information tables to stories

Category	**What**	**Protects from**
Authentication	Confirms the identity is who it says it is	The whole world
Access Controls	Provides additional authentication / validation to access specific resources	Compromised (stolen) Credentials
Authorization	Determines what actions the identity can perform on specific resources	Accidents, Compromised Credentials, Malicious Insiders

To counter the full range of threats, including accidents, we need a fully realized authorization model. This model must continuously learn from it's identities' activities and provide the proper authorization. This means analyzing your security with a distinct authorization layer in mind.

For the traditionalists among you who may think RBAC can still save the day, stay tuned for our next entry. (Spoiler Alert: It can't)