The Risks of Over Privileged Identities

There are four basic types of risks associated with over privileged identities and they all share the same key problem: a lack of understanding about what identities are doing in critical cloud systems and how those identities interact with crown jewel data.

Risk 1: Hacker's Delight

An attack based on privilege escalation is likely to be much easier if the point of entry is an account which already has a high level of privileges.

**Hackers Helper:** The easiest way to gain access is to create an employee with almost any permissions from your cloud service provider’s IAM resources, such as Amazon’s IAM. You can use the least-privilege principle to minimize the amount of data each identity can reach, and continuously monitor your critical data sitting inside object stores and database services.

**Malicious Entry:** A cloud resource or service with certain permissions may provide an easy entry point for further privilege escalation. Be sure to check that access has not been disabled.

**Standard:** Accepting default security settings may leave your entire system open to attack because these settings may have been changed by insiders or even a competitor who has access to your sensitive data.

Prevent unauthorized users from breaking hashes by continuously monitoring access across multiple cloud providers and 3rd party data stores. Use tools that allow you to see what is accessing that data, what has access, what could get access, and what has changed.

Risk 2: Accidents Will Happen

It’s easy to do damage when you’re operating in a technologically complex, sensitive area that can or should be off-limits, and this is when accidents happen with access and control.

**Invader:** Initial level of privilege may be adequate as an observer, but as soon as a new service requires access at a higher level, where they cannot be easily revoked, resource changes can be made that result in unauthorized access.

**Inflated:** Applications and services with elevated privileges are more common than you think. In addition to resource changes at the system level, many organizations allow services to access resources outside of their designated locations, or do so with protections.

**Misconfiguration:** Abusing existing privileges for malicious activity can be much easier. Malicious insiders can make changes to an existing service or interact with the system outside its designated location. If not properly monitored, they're easy to get access to and track down.

**ESCR:** It’s easy to do damage when you’re operating in technologically complex, sensitive areas that can or should be off-limits. Prevention can be tough, so finding and removing previously invisible risk is important. Add privacy and compliance controls to monitor across multiple cloud providers and 3rd party data stores. Use tools that allow you to see what is accessing that data, what has access, what could get access, and what has changed.

Risk 3: In Plain Sight

Human mistakes will happen and will not be deliberate at times, but these errors can still wreak havoc in an organization.

**Lackadaisical:** Employees who make minor mistakes in a permitted area. They have existing permissions where it is not adequately protected, or where it is not protected at all.

**Slothful:** Employees who take a shortcut, leaving sensitive data in a location where it is not adequately protected.

**Stupefied:** Employees who take an accidental leave, choosing a location where it is not adequately protected.

**Seized:** Any time a human user or intended resource is not set up properly, it is vulnerable to theft, or even to set up a competing business.

**Unsecured Access:** Every role human or system-based needs admin access, which should be protected, or where it is not protected at all.

Prevent accidents. Continuously monitor your critical data and map identities to find and remove visible and invisible identity risk. Add privacy and compliance controls to monitor across multiple cloud providers and 3rd party data stores. Coordinate with relevant industry leads to correct.

Risk 4: Insider Malice

The simplest and most common situation is when an insider uses legitimate permissions for malicious activities. We’ll look at some examples below. It is not easy to detect.

**Revenge:** Someone with sufficient privileges may use the need to access sensitive data to steal or manipulate data, and find a way to access it.

**Relate:** Someone with sufficient privileges may use the need to access sensitive data to steal or manipulate data, and find a way to access it.

**Stealth:** Someone with sufficient privileges may use the need to access sensitive data to steal or manipulate data, and find a way to access it.

Prevent insider threats. Detecting malicious activity can be tough, but finding and removing previously invisible risk can be even tougher. Detection of attacks, forensics, and separation of duty risks aren’t all covered by roles and responsibilities. You need to look beyond roles and responsibilities. You need to look beyond.

Taking Control

The best way to take control of your organization’s security and reign in overprivileged identities is by means of a comprehensive cloud-based security platform. This allows you to manage identity and data relationships at the ground level while integrating with your cloud service provider’s IAM resources.

With the right kind of platform and support, you can replace privilege inflation with privilege control and replace risk with genuine security.

Visit www.SonraiSecurity.com to learn more about public cloud security platform that provides a complete risk model of all identities and data relationships, including activity and movement across cloud accounts, cloud providers, and 3rd party data stores.