The Risks of Over Privileged Identities

There are four basic types of risk associated with over privileged identities and they all share the same key problem: a poor understanding of 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 unauthorized use of another user's account when an employee either purposely steals someone's credentials or obtains them by mistake.

Malicious Entry:
A cloud service or resource with inflated privileges may provide an even easier attack surface, particularly if it has a known default password which has not been disabled.

Standard:
Accepting default security settings may leave your entire system open to attack because basic provisioning may be the most widely-used resource and well known to potential intruders.

Prevent unauthorized users from wreaking havoc 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 technologically complex, sensitive areas that are or should be off-limits and this is when accidents happen with access and control.

Invader:
Inflated level of privilege may accidentally delete files or entire directories in a network environment where they cannot be easily recovered, or make changes to system settings (file associations, registry entries, DSNs) which render all or part of a system unusable.

Inflated:
Applications and services with inflated privileges may not be as clumsy as human beings, but they can still cause unwanted changes at the system level by doing such things as overwriting data which should be protected, installing incompatible versions of key resources, or redirecting user data to write-protected locations.

Misconfiguration:
Misconfigurations and snowflake configurations, whether they are the fault of overprivileged humans or resources, can be extraordinarily difficult to track down and fix.

Tired/Overworked:
Tired overworked project manager who occasionally needs admin access, and who knows better, but still writes passwords down on sticky notes.

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 DevOps teams to correct.

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 leave more than just passwords lying around. They leave sensitive data in locations where it is not adequately protected, or where it is not protected at all.

Slothful:
Employee who takes shortcuts leaving sensitive data in locations where it is not adequately protected.

Unauthorized Access:
Every role human or system-based that has unnecessary access to your customers' billing records, PII, etc. increases the probability that some of that information will eventually find its way onto a plain text file in full view of the public.

Prevent Accidents: Strictly enforce 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. See what is accessing that data, what has access, what could get access, and what has changed to prevent crown-jewel data loss. Also educate users about proper behavior and let them know they are being monitored.

Risk 4: Insider Malice

The simplest and most common situation is when an insider uses legitimate permissions for malicious activities. Malicious insiders come in a variety of flavors, and not easy to spot.

Revenge:
People may take a position with a company in order to gain access to sensitive data, and formerly trustworthy employees may become compromised.

Retaliate:
Former employees may want to retaliate for being fired, and even people who left under apparently friendly circumstances may want access to sensitive company data in order, for example, to sell it to a rival, or even to set up a competing business.

Stealth:
Someone with sufficient privileges and a reasonably good understanding of system security may be able to set up one or more overprivileged "sleeper" roles, allowing them to do an extraordinary amount of damage.

Prevent Insider Threats: Detecting malicious activity can be tough, so finding and removing previously invisible identity risk is important. Find a solution that can identify all excessive privilege, escalation, and separation of duty risks across 1000's of roles and compute instances across 100's of cloud accounts.

Taking Control

The best way to take control of your operation'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 a fine-grained 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 identity and data relationships, including activity and movement across cloud accounts, cloud providers, and 3rd party data stores.