

# LEADERSHIP BRIEF

## Privileged Account Management Considerations

Strong management of the use of the privileged accounts needed to manage IT infrastructure and applications is essential to protect against mistakes and misuse, as well as cyber-crime.

### 1. Recommendations

This document describes the management of the enhanced access needed to manage IT infrastructure, systems and applications. This enhanced access is usually provided through 'privileged' user accounts such as 'root' in UNIX. Increased privilege can lead to an increased impact if it is abused. Organizations need to take steps to manage this risk including:

- Implement a Privilege Management System.
- Control the use of shared accounts.
- Implement the principle of least privilege.
- Allow privileged access only when needed.
- Limit the scope of privilege where it is allowed.
- Implement segregation of duties.
- Use strong authentication for privileged access.
- Assure trust in how privilege is used.

### 2. Analysis

The management of the IT infrastructure upon which an organization depends requires access to maintain and configure the component systems and their security. This is a highly skilled activity that requires access to functions and components of the systems that are not available to normal users. To enable this access, IT systems, applications, and middleware provide built in accounts with the enhanced access needed. These are referred to as 'privileged accounts'. It is essential that these accounts - and their use - are carefully managed.

While these accounts are essential their abuse can have a high impact. Therefore, with privilege comes a greater need for trust; it is essential that steps are taken to assure this trust. Abuses of privilege can occur through malice, misuse or mistake: malicious abuse includes theft and criminal activities; misuse includes access through curiosity but without malicious intent; mistakes include damage due to erroneous use of management commands.

Cyber-criminals regularly target privileged accounts because these provide a route that allows them to take control over a system and gives unrestricted access to data.

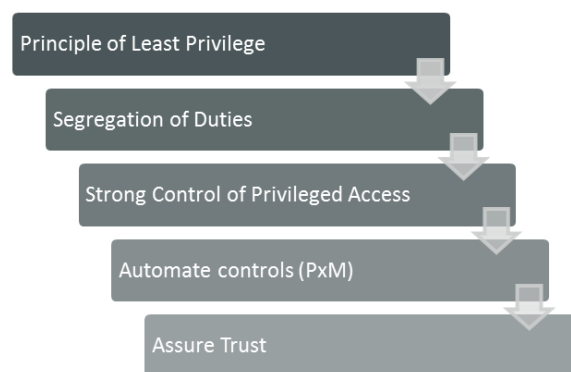


Figure 1: Privileged Account Management Overview

The following principles should be followed:

**Implement a Privilege Management System (PxM) covering all privileged accounts:** There are various marketing terms for these such as Privileged Account Management, Privileged Identity Management, and

Privileged User Management. In essence these are systems that automate and monitor the application of many of the following principles.

**Control Shared Accounts:** one critical vulnerability is that many systems provide only a single privileged account. This account must therefore be shared between administrators making it difficult to control and trace who did what. One way to achieve control over this is by keeping passwords to shared accounts in a vault and only releasing them as needed. PxM systems provide automation for this control.

**Implement the Principle of Least Privilege:** first defined in 1974<sup>1</sup>; this advises that both people and system components should only be given the access necessary to perform their job. Privileged accounts should not be used for normal day to day user activities.

**Allow Privilege only when needed** - limit privileged access to the short period of time that it is needed to allow a specific person to perform a defined task. This approach provides greater control over and accountability for the use of a privilege account.

**Limit the Scope of Privilege** – use processes and / or technology to provide a more granular control of access. For example, incorporate technology that allows a systems administrator to perform legitimate administration but not to access application data.

**Implement Segregation of Duties:** There should be a clear delineation between the creation and approval of a change request and the implementation of the changes. That is to say the administrator with privileged access must not be able to unilaterally request and approve a change as well as to make that change.

**Implement Strong Authentication:** Privileged accounts should require the strongest authentication possible within the system. This makes it more difficult for cyber-criminals to gain privileged access and provides extra assurance over the identity of the administrator. Two factor authentication is recommended as the minimum.

**Assure Trust:** The greater the privilege the more the need to assure trust in the way it is used.

- **Vetting:** Perform background checks on individuals given privileged access. This is to protect against organized crime or competitors planting people with the objective of gaining illegitimate insider access. It is also to protect against the risks of staff being blackmailed.

**Activity Monitoring** – to assure trust in the way privileged accounts are used organizations should ensure that that all activities using these accounts are logged and that these logs are monitored.

### 3. Summary

Managing the use of privileged accounts is essential to protect against mistakes and misuse as well as cyber-attacks and leakage of data. Organizations need to take steps to manage privilege by implementing the

principle of least privilege, segregating administration from change requests approval, automating strong controls using PxM tools, and take steps to assure trust in how privilege is used.

## The Future of Information Security – Today

  2015 Kuppinger Cole Ltd. All rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks<sup>TM</sup> or registered<sup> </sup> trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

<sup>1</sup> Saltzer, Jerome H. (1974). "Protection and the control of information sharing in multics". Communications of the ACM 17 (7): 389