Introduction

Why PAM?

Privileged Account Management (from this point forward: PAM), allows you to manage accounts that are necessary to perform scheduled configuration and maintenance tasks, as well as supervening tasks such as the recovery of a hardware or software failure or the restoration of a backup. Due precisely to the need to use these accounts in an unplanned manner, their management must combine security, procedures and flexibility. PAM is the process of determining who has access to what types of information as it creates an integrated view of risk, threats, and controls.

PAM is considered by many analysts and technologists as one of the most important security projects for reducing cyber risk and achieving high-security ROI.

PAM Goals

Reduce the attack surface

- Have an up to date global catalog of accounts and permissions.
- Close the gap between the user and administrator accounts.
- Assign the ownership and responsibilities for each account.
- Complex and rotated passwords.
- Use strong autentication.
- Track accounts ownership and warns when an account loses its last owner.

Minimize the potential impact

- Rectification campaigns to confirm the permissions assigned to each service account.
- Apply dynamic authorization engine (XAML) to grant access to critical resources.

Rapid attack detection

Detection phase

- Exexecution of dangerous commands.
- Usage of dangerous applications.

Response actions

- Drop offending session.
- Lock account.

Notification

- Account owner notification by SMS/Email.
- Creation of a ticket.

Generate and keep legal evidence

- Record privileged account sessions (Screen, KeyBoard, Clipboard, and File transfers).
- Keep encrypted in a secure storage.

Revision #9
Created 13 July 2021 10:25:27
Updated 1 December 2022 11:44:11