IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

IJARSCT

Impact Factor: 7.301

Volume 3, Issue 1, July 2023

Privileged Access Management: Ensuring Security and Accountability

Mr. Siddhesh Bhargude
Student, Master of Computer Application
Late Bhausaheb Hiray S.S. Trust's Institute of Computer Application, Mumbai, India

Abstract*: An essential security strategy known as Privileged Access Management (PAM) focuses on monitoring and controlling access to critical internal systems, networks, and data. This research paper provides a comprehensive overview of Privileged Access Management, examines its relevance for modern cybersecurity, and lists the key principles and components needed to develop an effective PAM program. The research also discusses the benefits and drawbacks of PAM and provides deployment best practices. Through a detailed investigation of the body of prior research, industry reports, and case studies, the study offers insights into the current state of PAM and predicted changes.*

Keywords: PAM, authorisation, authentication, compliance, and risk management

I. INTRODUCTION

Privileged access management (PAM) is a crucial component of modern cybersecurity approaches. As businesses increasingly rely on digital systems and networks to store and process sensitive data, the security of privileged accounts becomes essential. Privileged accounts, or users with elevated access privileges and permissions, have access to sensitive information and can perform essential functions as well as change the entire system. These advantages, however, might come with significant risks if they are not properly managed and supervised.

Privileged Access Management: A Short Introduction

The practices, standards, and resources utilized by an organization to manage, secure, and limit access to privileged accounts are referred to as privileged access management (PAM). By restricting access to privileged accounts to those who are authorized and have a legitimate need for them, PAM aims to lessen the risk of misuse, abuse, or unauthorized access. Privilege account discovery, credential management, access control, session monitoring, and auditing are PAM systems' constituent parts.

By implementing PAM, organizations can establish a comprehensive framework for controlling privileged access, maintaining accountability, and lowering the risk of security breaches. PAM solutions give organizations comprehensive control over privileged accounts, allowing them to create and enforce least privilege policies and ensure that individuals only have the access privileges required to do their specific tasks. PAM helps organizations comply with compliance and regulatory requirements by providing complete audit logs, monitoring privileged sessions, and enforcing strong authentication and authorization procedures.

The importance of Privileged Access Management cannot be overstated. Numerous high-profile security breaches in recent years have been attributed to hacked privileged accounts. Attackers target these accounts because they grant them access to the organization's most vital resources, enabling them to move across the network, gain more privileges, and exfiltrate sensitive data.

PAM's importance and relevance in contemporary cybersecurity

1. Protection from Insider Threats: Insider threats pose a severe risk to organizations, whether they are deliberate or unintentional. PAM aids in lowering these risks by putting in place strict restrictions and monitoring mechanisms for privileged accounts.

2. Privileged accounts are commonly targeted by external attackers that want to gain unauthorized access to sensitive data and important systems. This process is referred to as "mitigation of external threats." PAM offers a powerful

DOI: 10.48175/IJARSCT-12098

defence against these risks by respecting the concept of least privilege and guaranteeing that users have only the access required to fulfil their duties.
3.Compliance and regulatory standards impose strict management and oversight of privileged accounts on organizations in a range of industries.

Privileged Access Management Definition and Purpose

For controlling, safeguarding, and limiting access to privileged accounts within an organization's IT infrastructure, Privileged Access Management (PAM) is a group of protocols, rules, and tools. Due to their greater access privileges and permissions, privileged accounts enable users to perform significant actions,
change the entire system, and access confidential information.

The following significant elements are included in the scope of privileged access management.

1. The aim of privileged account discovery is to identify and catalog all privileged accounts that are present in the company's IT infrastructure. You must be familiar with user accounts, service accounts, administrator accounts, and other privileged credentials in order to accomplish this.
2. The practice of managing privileged account credentials by implementing secure procedures is referred to as credential management. This necessitates practices like safe storage, encryption, rotation, and strong password restrictions in order to ensure the integrity and confidentiality of privileged credentials.
3. Access Control: To limit privileged access, granular access restrictions are built using the principle of least privilege. By ensuring that users only have the privileges required to fulfil their individual jobs, access control systems reduce the risk of unauthorized access and misuse.
4. Session monitoring and auditing refers to the use of technologies to observe and record the actions of privileged users during their sessions. This involves recording commands and operations, capturing session data, and creating audit trails for forensic investigations and compliance requirements.
5. Putting into practice the notion of "just-in-time access," where users are given authorization for a particular task or length of time. By making sure that privileges are only accessible when necessary, this reduces the vulnerability of sensitive resources.

Privileged accounts' function in ensuring organisational security.

1. Privileged accounts are typically granted to system administrators, network administrators, database administrators, and other IT staff members who are in charge of monitoring and maintaining important infrastructure components
2. Access to sensitive data, including customer information, proprietary information, financial data, and other irreplaceable assets, is regularly granted to privileged accounts.
3. System Configuration and Changes: Privileged accounts are necessary for configuring and making changes to an organization's computer and network systems. They have the authority to change system settings, install software patches and upgrades, and make changes that have an impact on the level of general security.
4. Privileged accounts within an organization are in charge of managing user rights and access permissions. They are able to create and modify user accounts as well as assign rights and determine user roles.
5. Forensic investigations and incident response: Privileged accounts are routinely utilized in the incident response process when there are security events or breaches. They are responsible for carrying out forensic investigations, examining logs, and identifying the root causes of security problems.

Privileged access management's significance

1. Protection from Insider Threats: Insider threats pose a severe risk to organizations, whether they are deliberate or unintentional. To lessen these dangers, PAM uses strong controls and monitoring mechanisms for privileged accounts.
2. Defense against External Attacks: External attackers routinely target privileged accounts in an effort to obtain unauthorized access to sensitive data and crucial systems. PAM offers a powerful defence against these risks

DOI: 10.48175/IJARSCT-12098

by respecting the concept of least privilege and guaranteeing that users have only the access required to fulfil their duties.

3. Compliance and regulatory requirements impose strict controls and monitoring of privileged accounts on organizations in a range of industries. PAM systems provide the necessary auditing and controls to meet these requirements
4. Better Accountability and Auditability: PAM enables organizations to establish strict accountability requirements for privileged acts. PAM systems integrate features like session monitoring, activity logging, and auditing to provide a comprehensive record of privileged operations.
5. Mitigation of Credential-based Attacks: Credentials continue to be a popular target for hackers. To safeguard the credentials for privileged accounts, PAM enforces strict authentication and access control policies.

Benefits of Privileged Access Management

1. Scalability and Flexibility: PAM systems are designed to adapt to the shifting demands of business as well as the shifting landscape of IT. They provide scalability and flexibility to manage complex IT settings, including cloud-based systems, third-party integrations, and remote access requirements.
2. Lessened Insider Threats: Insider threats can represent severe risks to organizations, whether they are deliberate or unintentional. PAM lowers these risks by implementing strict supervision policies and controls for privileged accounts.
3. Because PAM's reduced privileged access procedures reduce administrative costs and promote operational effectiveness, productivity and operational efficiency are increased. PAM systems offer centralized administration, automated privilege procedures, and self-service capabilities, enabling authorized users to obtain privileged access quickly and efficiently.
4. Productivity and operational effectiveness are improved as a result of PAM's streamlined privileged access procedures. Operational efficiency is increased while administrative expenditures are reduced. PAM systems enable authorized users to get privileged access quickly and effectively by providing centralized management, automated privilege procedures, and self-service capabilities.
5. Enhanced Security and Protection: PAM adds a robust layer of security for privileged accounts. It implements strict authentication requirements, such as multifactor authentication, to guarantee that only authorized users may access privileged credentials. PAM systems follow the least privilege principle as well, granting users only the privileges necessary to complete the job at hand.

Challenges of Privileged Access Management

1. Complexity and Implementation Effort: It could be difficult to integrate PAM systems into the current IT architecture. When establishing proper access controls, comprehending and mapping their privileged accounts, and configuring the PAM solution to suit their particular requirements, organizations may run into challenges.
2. PAM makes an effort to establish stringent security restrictions, but it should also consider the usability and productivity of privileged users. Finding the perfect balance between security and usability may be challenging.
3. User Resistance and Adoption: User behavior and workflow frequently need to change when PAM solutions are implemented. Some powerful users may object to the adoption of PAM because they believe it will make them less productive or add more authentication steps.
4. Privileged Account Sprawl: Companies may find it challenging to identify and manage all of the privileged accounts in their IT ecosystem. The existence of privileged accounts can occur in a variety of settings, programs, and platforms, making it challenging to create a precise inventory.
5. Access revocation and Privilege Creep: Privilege creep happens when privileged users accumulate unnecessary privileges over time. Making sure that rights are swiftly revoked when they are no longer needed might be challenging.

DOI: 10.48175/IJARSCT-12098

Case studies and real-world example on privileged access management

The first case study is Target Corporation.

Millions of consumer credit card numbers were stolen from Target Corporation in 2013 as a result of a serious security breach. The incident took place when hackers gained access to Target's network using credentials they acquired from a third-party supplier. This incident drove home the importance of privileged access control in preventing unauthorized access to critical systems and data.

Using a potent Privileged Access Management system following the incident, Target Corporation improved their security posture. Strict access controls, dependable authentication protocols, as well as session auditing and monitoring for privileged accounts, were all implemented. With the help of the PAM system, Target was able to manage and monitor privileged access, reducing the possibility of further accidents. The Target Corporation example demonstrates the importance of PAM in preventing external attacks and protecting private customer information.

The second case study of Sony Pictures Entertainment

Private data, including sensitive company documents and staff emails, were stolen and leaked as a result of a well-known cyberattack that attacked Sony Pictures Entertainment in 2014. A group of hackers were blamed for the incident because they broke into the business's network using stolen privileged credentials.

After the attack, Sony Pictures Entertainment implemented Privileged Access Management to strengthen their security protocols. PAM systems were used to implement the least privilege principle, manage and monitor privileged accounts, and enable multi-factor authentication. These safety measures helped Sony Pictures Entertainment reduce the potential harm from insider threats and limit access to key systems.

The situation involving Sony Pictures Entertainment emphasizes the importance of PAM in protecting against both internal and external threats. By implementing PAM, organizations can strengthen their security posture and reduce their risk of unauthorized access and data breaches.

II. CONCLUSION

Privileged Access Management (PAM) is crucial for upholding security and accountability within organizations, to sum up. PAM uses stringent controls, monitoring software, and access control methods to handle the issues caused by privileged accounts. PAM reduces the risk exposure of organizations by controlling privileged access and reducing the chance of unauthorized access, account misuse, and abuse. PAM enhances security and protection by imposing strict authentication procedures, adhering to the least privilege principle, and ensuring that only authorized users with a legitimate need can access privileged credentials and carry out privileged operations.

PAM improves compliance and accountability with robust auditing and monitoring features that generate detailed logs and audit trails of privileged activities. This enables organizations in demonstrating compliance with industry laws, supports forensic investigations, and encourages compliance. PAM boosts operational effectiveness and productivity by automating privilege operations, centralizing administration, and providing self-service choices. This eliminates useless delays and obstacles, enabling authorized users to obtain privileged access quickly and effectively.

Privileged Access Management is a crucial component of a comprehensive cybersecurity strategy, to sum up. It helps organizations safeguard important systems, networks, and data by enforcing stringent security regulations, reducing risks, and ensuring accountability for privileged access. PAM can assist businesses in enhancing their security posture, adhering to rules, and guarding against insider threats, all of which will ultimately result in a more secure and resilient online environment.

REFERENCES

[1]. 2018; Bejtlich, R. Building Effective Cyber-Defense Strategies to Protect Organizations: Privileged Attack Vectors. Media by O'Reilly.

[2]. R. A. Caralli and P. Gallagher (2014). A Architectural Approach to Securing Privileged Accounts is Privileged User Management. Carnegie Mellon University's Institute for Software Engineering.

DOI: 10.48175/IJARSCT-12098

[3]. Goel, S., Brar, G., & Goel, (2017). What is Privileged Access Management and why do you need it? The RSA Conference.

[4]. J. Haber, R. Rudolph, et al. Managing Privileged Accounts for Novices. Wiley & Sons, Inc.

[5]. The Ponemon Institute. The PAM (Private Access Management) Report for 2020.

[6]. SANS Institute, 2020 [6]. Implementation Guide for Privileged Access Management (PAM).

[7]. David Servon (2016). A Practical Approach to Managing Privileged Accounts and Processes: Privileged Identity Management. Apress.

[8]. J. Shapero, C. Hsieh, et al. A Buyer's Guide to Modern Privileged Access Management. Gartner.

[9]. NIST, the National Institute for Standards and Technology, 2020. Security and privacy controls for information systems and organizations are covered in NIST Special Publication 800-53.

[10]. Thycotic (2019), Privileged Access Management (PAM) Risk and Compliance Report: Global State.

DOI: 10.48175/IJARSCT-12098