ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 3, pp: (35-38), Month: July - September 2021, Available at: www.researchpublish.com

Prevent Unauthorized Access/Change Activities on Information Technology (IT) during COVID-19 pandemic lockdown

Abdullah M. Al-Shaikh , Khalid A. Al-Khathlan

Dhahran, The Kingdom of Saudi Arabia

Abstract: **The global experiences during the COVID-19 pandemic lockdown has suddenly created a huge demand and accelerated the investment at an unprecedented scale toward technologies that support off-premises workplace. The demand for strong remote access management has never been so great, especially for privilege users who need perform administrative operations from home or third-party.**

This article will shed light on practical recommendations that will help to enhance the IT change management process in alignment with information protection to prevent unauthorized change activities on information technology infrastructure. The recommendations will help to eliminate business interruption due to unplanned or unauthorized changes activities and will minimize/eliminate the impact in case of a cyber-attack.

Keywords: **COVID-19, PAM, IAM, Just-in-time, JIT, Cyber-Attack, IT Change Management, . Information Security, Risk Management.**

I. INTRODUCTION

Only a very few organizations have a workable business continuity plans for a pandemic incident of global scale. The accelerated shift from working on-premises to off-premises workplace during the COVID-19 pandemic lockdown has suddenly created new challenges. That cause a widespread concern especially with regard to the remote privileged access to fill gaps in security control that are not accomplished though legacy remote access SSL VPN, zero-trust network access (ZTNA) or cloud access security broker (CASB). That raised the additional requirement to enhance the privileged access management (PAM) solution. Quite often, adopting the new tools and technologies to support remote access don't meet with identity and access management (IAM) compliance requirements and need to be complemented by additional controls to mitigate remote-access-associated security.

Cybercriminals are most likely targeting large company's IT critical systems, industrial control systems and stole data. Privileged users hold the keys for those systems and data. Therefore, privileged users are often the primary targets of cyber-attack and are responsible for major breaches. In addition, privileged accounts are subject to perform unauthorized and undocumented changes that could harm IT Infrastructure and might cause unplanned business interruption.

Therefore, the importance to review and enhances privileged access management (PAM) solution become of great importance and unneglectable. Information Security and risk management team need to review IAM process especially with regard to the remote privileged access and elevate the PAM solution to safeguard the organization.

II. BACKGROUND

Privileged access assignment is usually performed by identity governance and administration (IGA). Privileged access management (PAM) systems interact with IGA tools to track life cycle for privileged user accounts. PAM systems may also interact with other tools to revoke privileges, activation or deactivation user account. It provides visibility and governance to track and monitor life cycle for privileged user accounts. PAM requires a strategy that includes the right people, processes, and technology.

III. ENHANCE PRIVILEGED ACCESS MANAGEMENT (PAM)

Privileged accounts are often the primary targets of cyber-attack and are responsible for major breaches. In addition, they are subject to perform unapproved changes activities that could harm IT Infrastructure and might cause unplanned business interruption. Therefore, privileged accounts deserve special attention and consideration. A mature PAM solution help to effectively mitigate and manages the risk of privileged accounts. To achieve these goals, PAM typically provides the following:

- Govern and control privileged user accounts on multiple systems.
- Establish controls for privileged account, shared accounts and emergency access for privileged accounts.
- Provide single-sign-on (SSO) for privileged accounts.
- Monitor and log all privileged access activity
- Provide just-in-time privileged access management.

Some organizations fail to implement the basics functions of PAM and others struggle to pursue the maturity in their PAM solution. Mature PAM solution is achieved by enforcing effective controls such as just-in-time (JIT) approaches through automation and integration with other enterprise tools. This section will shed the light on some recommendation to have a mature PAM solution that capture effective control to track, govern, control, log and monitor the privileged accounts activities to effectively mitigate privileged accounts remote-access-associated security risks. The controls and measures need to be proactive and reactive that cover both internal and external threats which may happen intentionally or unintentionally.

A. Establish a Remote User Identity Governance and Administration (IAM)

Create a special user identity for every privilege user in an organization IAM system. This is to enforce special user activation and authentication every time they intend to perform administrative tasks or privileged operations. Privileged user activation requests need to mandate a valid change request or trouble ticket to activate IT admin accounts within the approved time window. The solution needs to consider emergency situation and admin users who are required to perform daily operation or health checks that doesn’t alter any component within IT infrastructure. Those users should be configured with the least privileges.

B. Just-in-time (JIT) approach

Just-in-time approach is accomplished by granting the required privileges to the required system and to the right privileged account for the valid reason at the right time. PAM solution needs to provide an interface where administrators can request an activation or deactivation for their special privileged account. The solution must follow the just-in-time (JIT) approaches where privileged account are activated only when absolutely necessary with a valid change request or trouble ticket with zero standing privileges (ZSP) as the goal. In Fact, Gartner predicts that by 2024, 50% of organizations will implement a just-in-time (JIT) approaches, which removes permanent privileges, experiencing 80% less privileged breaches than those that don’t [2]. The purpose of a a just-in-time (JIT) model with zero standing privileges (ZSP) is to reduces the risk of privileged access abuse to perform unauthorized activities, and reduces the cyber-attack impact on the privileged accounts themselves.

C. Integrate PAM with IT service management (ITSM):

Just-in-time approach should be established through PAM solution integration with ITSM enterprise ticketing system (e.g. BMC Remedy or ServiceNow). The integration will enable PAM solution to mandate and validate having a valid change request or trouble ticket before submitting user activation requests for IT admin accounts. The admin accounts need to be assigned to a valid task within an approved change request or a trouble ticket or prior to submitting an Admin account activation request. The account activation needs to match the change window and not exceed the maximum time threshold. This integration will minimize unauthorized change activities on the IT Infrastructure and eliminate unplanned interruption to the business.

D. Monitor and log all privileged activity

The PAM solution should provide reports for analysis for all admin account activation requests that are associated with change requests, and monitor the daily operation and health check activation requests.

E. Multi-factor authentication:

Remote users' access should use Multi-Factor Authentication (MFA) to connect to the PAM system. The PAM solution should support two-factor authentication. The requester need receive a onetime password using mobile-based OTP, email passwords, physical keys that needs to be provided to the application as a second factor authentication.

F. Privilege access alerting notification:

In addition, the PAM solution should have the ability to notify security administrators system/data owners and authorized parties for any high-risk events, remote access, activation and deactivation of privilege account, requesting new permission, permission expiration and any altering of the status of privileged account using appropriate notification mechanisms such as reports, email, text messages, or other systems.

G. Privileged account and session management (PASM):

Privileged session management (PSM) is a class of PAM solution to grant administrators a temporary privileged access and ensure the accounts or session are enabled only for a specific predefined period of time and then account deactivated or session terminated if not renewed. PASM solutions can provide service-to-service password management, zero-install remote privileged access features for IT staff and third parties that do not require a VPN.

JIT can go deeper with PASM, for example, an admin account receives additional permissions one-time with just the right set of permissions for limited time frame and session. Those permissions are then removed.

H. Do not share admin accounts

Administrators should have a unique user identity (special account) to perform administrative work. They need to be unique for each administrator and different from the individual user account for day-to-day work. Those identity need to be assigned to individual administrators and not shared.

I. Privileged access request approval

In many organization, privileged accounts have a full permanent access to everything with no limit. To minimize risk, the PAM solution must ensure administrators gather only the minimum privileges needed to perform their jobs through access requests and secure the necessary approvals. Any privileged user permission should be requested and approved by authorized person who control the privileged account permission. and system/data owners

J. Ensure the PAM solution Service Continuity:

The PAM is a crucial system and must be deployed in a highly available manner and ensure having a business continuity strategy and disaster recovery solution. The service high-availability and business continuity options should cover all PAM service dependency. This includes network, applications, clustering severs, load balancers, storage, backup and all service dependency. Disaster recovery solutions must ensure service availability in case of total data centre loss or shutdown.

IV. CONCLUSION

Most organizations implement Digital Business Models that leverage deeply on information technology to run their business. Cybercriminals continue to be a potential exposure targeting large company's IT critical systems and data. Privileged users hold the keys for those systems and data. The privileged accounts are primary targets of cyber-attack and in sometimes are responsible for business interruption due to unplanned or unauthorized changes activities. The risk associated with privilege accounts has significantly increased during the global COVID-19 pandemic lockdown due to remote access permission. Additional controls need to be applied for privileged user with Remote Access permission. The implementation of a mature

To properly mitigate the risk of privileged account remote access associated risk, leaders in access management and security and risk management (SRM) recommend implementing a PAM solution with effective controls to trac, govern, control, log and monitor the privileged accounts. PAM soloution need to be leverage zero standing privileges strategy through a JIT approach, session management PASM and the integration with ITSM enterprise ticketing system (e.g. BMC Remedy or ServiceNow) to achieve

REFERENCES

[1] IAM Leaders' Guide to Privileged Access Management Published 15 February 2021 – Gartner ID G00738624 - By By Abhyuday Data, Felix Gaehtgens, Michael Kelley.

[2] Magic Quadrant for Privileged Access Management Published 4 August 2020 - Gartner ID G00381092 -By Felix Gaehtgens, Abhyuday Data, Michael Kelley

[3] Remove Standing Privileges Through a Just-in-Time PAM Approach (gartner.com) Refreshed 21 June 2021, Published 6 September 2019 - Gartner ID G00389807 By Michael Kelley, Felix Gaehtgens, Abhyuday Data