Journal of Engineering Sciences

Vol 11, Issue 5,May/2020
ISSN NO:0377-9254

A Review for the Risk, Threat and Mitigation of Unauthorized Access of Accounts

Deepak Kumar
M.Tech. Research Scholar
Department of CSE/IT
Noida International University

Dr. Bharti Kalra
Assistant Professor
Department of CSE/IT
Noida International University

Abstract: This review paper provide a broad overview of Risk and Threat involved for unaudited unauthorized users within an organization. Initially computer systems had low security and there was less probability of cyber threat as well. But with the increase of data over internet and cloud system, the importance of data and its security was truly realized [4]. In the beginning data was consider to be useful but not something that to be protected from unauthorized access.

The internet is evolved as amazingly useful and versatile tool that has become indispensably, while taking care to protect yourself and your data and you will continue to find it a valuable resource. A proper monitoring and Auditing of unauthorized windows account can protect our data from unauthorized access. Identity Lifecycle management is the most important part to protect data[16]. A terminated or inactive accounts must not have active windows account to login. Which an unauthorized user can use to login and steal important data of organization [15].

Keywords: - Auditing Users Lifecycle, Active Accounts for Inactive Users. Unauthorized Access Threat, Terminated User Accounts. Account Certification.

I. INTRODUCTION

Identity Life Cycle Management: Identity Life Cycle Management is very important tool now a days which can help to monitor and audit users within an organization[15]. These tools focuses to manage users of an organization from there onboarding to terminations within the system. During the life cycle of an Identity it keeps track of assets available to the identities and accesses available to the users. These are being used to protect data from unauthorized access, change or destruction. Government, military, hospitals and other businesses. With the growing volume and sophistication of cyber-attacks. Ongoing attention is required to protect sensitive business and personal information as well as safeguard national security [8].

In this review we are trying to mitigate the threat raised because of unauthorized account at Source, which is major threat for the organization and very high risk to the data.

The internet is evolved as amazingly useful and versatile tool that has become indispensably, while taking care to protect yourself and your valuable data [9]. A proper monitoring and Auditing of unauthorized windows account can protect our data from hacker. There are top 6 cyber-security actions. To protect the data we use personal Firewalls, Prevent Identity Theft, Run Anti-virus Software, Avoid Spyware, Protect Passwords, Back up Important Files and Most Important is to protect data from the users which were part of the security system but now no longer exist and must be prevented to login into the system.

Figure 1: Lifecycle of an Identity

II. LITERATURE REVIEW

Until today, there has been a lot of work and review done to protect the data from the outsider and hackers [5]. With the growing threat of data security internal users are also a major threat to privacy and data is not any proper way to monitor the inactive accounts and their licenses [6]. It is still a manual process by Active Directory and Windows team to monitor such terminated or deprovisioned users within organization[8]. A broad review was done by Mark Russinovich, Byron Hynes[3] and other researcher to manage users account on windows server.

II. A. Prior Work

Microsoft has itself developed many tools to manage the users and their lifecycle within their domain. Later SolarWinds, ManageEngine and WiseSoft [4] created their own customized tools to manage and perform individual task within the platform like account auditing, password management and bulk user management [6].

Disadvantage of all these solutions are like they can only look for the data within their platform only and they need to be depended on the data provided to them by HR system and later they can manually verify or validate users access or license on Active Directory side.

As per existing architecture HR system like workday sends users onboarding and off boarding details to IDM and Active Directory and they perform the process to make the users active or inactive.

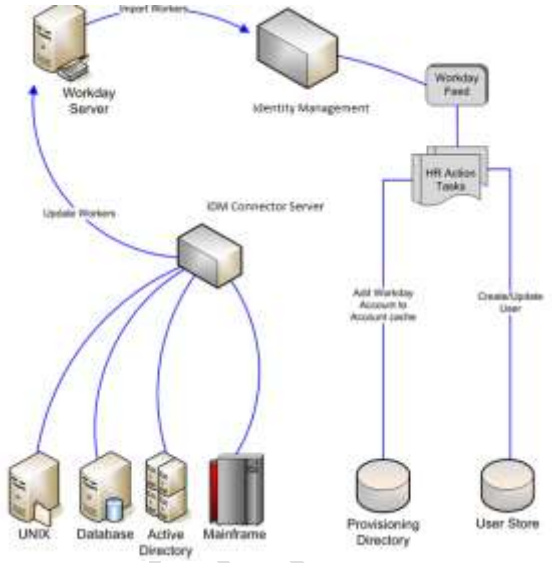

Figure 2: Existing User Management Process

Major drawback of the process is unaudited users at active directory i.e. at source. In case of any technical failure in the process can leave the account active at the Active Directory[7]. Such users are big threat to the organizational data. They can login to the system even after their terminations and they can steal sensitive information.

Sailpoint [15]: - Now a days Sailpoint is one of the most trending IDM tool which is being used to manage user's lifecycle within the organization. It's Governance and Reporting tools can be used to provision - deprovision and audit the users' access over the system. Sailpoint group provisioning features can be used to track the license for active directory accounts.

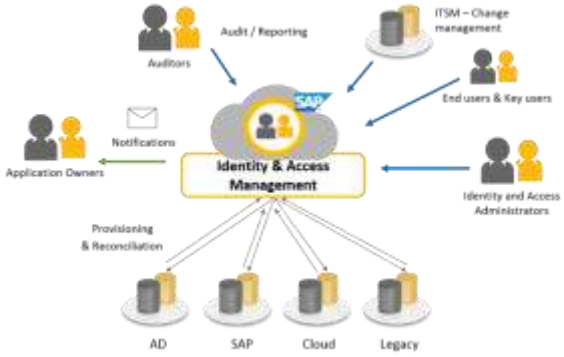

Figure 3: Account Management by IDM

These access management tools can be effectively used to track provisioning and terminations of account. We can leverage the facilities and it can be enhanced to implement the functionality to monitor/audit terminated user using an active AD users groups.

III. PRESENT WORK

Identity Management Tools like Sailpoint facilities can be enhanced to leverage the governance module to properly audit the user's accounts after their termination from the organization. Following are the enhancement and functionalities added in the work:-

i) Proper account certification and review process
ii) Group based Active Directory license process to audit users
iii) Time based email notification process to verify accounts
iv) Remove accounts from license groups

Above mentioned approach provide double layered security, which can help to identify unauthorized users within the organization and the security risk can be removed or mitigated easily.

A new AD license group which is managed by Identity Management Application [3]. Our new implementation will look for all users under the license group against their employment status in Identity Management Application. It will help us to identify possible threat like users terminated in HR System but still active accounts to login.

Once identifying the possible security threats a notification to the manager of account owner is sent to verify and user is removed from license group and account is deactivated.

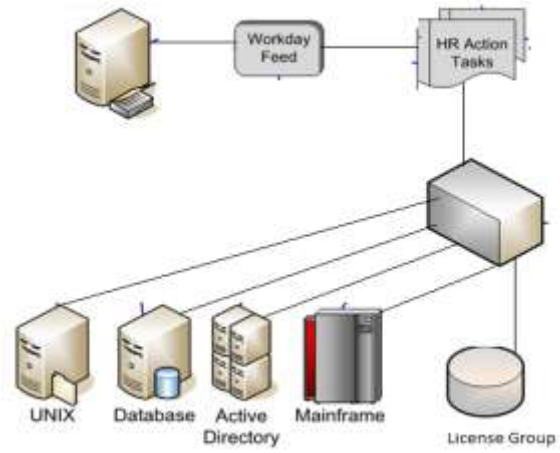

Figure 4: Current Flow and User Management

In the current work we have enhanced IDM application to use additional license group to keep track of internal users within the organization. This group will be validated against user's employment status in IDM application and any discrepancies will be fixed after notification.

Current work will validate users' status in License group and IDM application and based on users status in HR system there access will be revoked or granted and a notification to the owners manager will be triggered for information.

IV. CONCLUSION AND FUTURE WORK

In this paper we have tried to implement more effective process to audit internal unauthorized users. We have used better technique and process to mitigate the threat for internal process. We have tried to overcome the existing issues and used better technique and implementation plan which includes effective account certification, new implementation to monitor internal users' access using new license group.

This review paper provides a novel solution to mitigate the threat raised within an organization due to unauthorized access.

V. REFERENCES

[1] "Directory System Agent". MSDN Library. Microsoft. Retrieved 23 April 2014.

[2] Solomon, David A.; Russinovich, Mark (2005). "Chapter 13". Microsoft Windows Internals:

Microsoft Windows Server 2003, Windows XP, and Windows 2000 (4th ed.). Redmond, Washington: Microsoft Press. p. 840. ISBN 0-7356-1917-4.

[3] Hynes, Byron (November 2006). "The Future Of Windows: Directory Services in Windows Server "Longhorn"". TechNet Magazine. Microsoft.

[4] "Active Directory on a Windows Server 2003 Network". Active Directory Collection. Microsoft. 13 March 2003. Retrieved 25 December 2010.

[5] "Install Active Directory Domain Services on Windows Server 2008 R2 Enterprise 64-bit". 27 April 2016. Retrieved 22 September 2016.

[6] "The LDAP Application Program Interface". Retrieved 26 November 2013.

[7] "An Approach for Using LDAP as a Network Information Service". Retrieved 26 November 2013.

[8] "The Lightweight Directory Access Protocol (LDAP) Content Synchronization Operation". Retrieved 26 November 2013.

[9] Thomas, Guy. "Windows Server 2008 - New Features". ComputerPerformance.co.uk. Computer Performance Ltd.

[10] "What's New in Active Directory in Windows Server". Windows Server 2012 R2 and

[11] Stroud, Forrest. "What Is Identity and Access Management (IAM)? Webopedia Definition". www.webopedia.com. Retrieved 27 February 2019.

[12] "IdenTrust Home | IdenTrust". www.identrust.com. Retrieved 27 February 2019.

[13] Compare: "Gartner IT Glossary > Identity and Access Management (IAM)". Gartner. Retrieved 2 September 2016. Identity and access management (IAM) is the security discipline that enables the right individuals to access the right resources at the right times for the right reasons. [...] IAM addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet increasingly rigorous compliance requirements.

[14] “Identity management (ID management)". SearchSecurity. 1 October 2013. Retrieved 2 March 2017.

[15] "What is identity management (ID management) ? - Definition from WhatIs.com". SearchSecurity. Retrieved 20 December 2019.

[16] "System for Cross-domain Identity Management: Core Schema". *ietf.org*. Internet Engineering Task Force. September 2015.