ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 3, pp: (251-252), Month: July - September 2020, Available at: www.researchpublish.com

Identity and Access Management Lifecycle

[1]Taher A. Alwusaibie

[1]Saudi Aramco, Dhahran, Saudi Arabia

Abstract: **Identity and Access Management (IAM) plays an integral part in the overall cybersecurity posture of any enterprise. In this area, simply deploying an IAM solution will not ensure that your enterprise is following best practices in this cybersecurity pillar. Most products in the market provide many of the functionalities that businesses require. Employing these features and functions, and translating them into the right method to protect assets, is what matters the most.**

This paper aims to identify the common cybersecurity practices in the area of IAM lifecycle to ensure that users and identities are managed with least privileged model in-place. The paper discusses IAM concepts that the enterprise should maintain, to secure their identity and access management, as any wrongdoing in this area can have severe impact.

Keywords: **Identity and Access Management, IAM, Lifecycle Management.**

1. INTRODUCTION

Identity and access management (IAM) is the area that enables the right users to access the right resources at the right time with the proper business needs. In concept, IAM might be manageable in a small company with 100 or less users, because the IAM lifecycle can be handled manually. As organizations grow larger, they will need to consider the right tools and automation, and implement them with the correct controls, to have an effective access and authorization management lifecycle.

2. IDENTITY PROVISIONING

The first thing that needs to be considered is the onboarding process of a user. Your company is hiring on a daily or monthly basis, and you need an automated way to ensure your users have default access to start their work. To accomplish this part, you need to identify the systems that new users require which in many cases at minimum will need an HR system, Active Directory and Exchange. To enable a fast on-boarding process, you need to identify with the business units what exactly new users need for each business function. For example, a newly hired help desk agent will need to be granted access to the service management system such as ServiceNow. Mapping these out for all business units will enable you to embrace a powerful onboarding process of new users.

3. IDENTITY DE-PROVISIONING

This is referred to as the separation of an employee, contractor or consultant, etc., where you need to immediately act on their accounts and access to ensure proper termination of all associated privileges. Users will definitely build up their access profile over time, and this could be difficult to take care of if not all systems are governed by your IAM overall process. For example, users might have a local account created on a computer that they could abuse, even after their domain account is deactivated. In addition, they could have copies of credentials for service accounts used in the environment, as part of their previous roles and responsibilities.

Therefore, the de-provisioning process is critical to closing the lifecycle of an identity. It is even more concerning if your users have been separated due to unforeseen and unexpected circumstances, such as a layoff program. So, this step must be thought of carefully to ensure users no longer have access to any resources after they are terminated.

4. ACCESS REQUESTS

Over the lifecycle of an identity, a requesting mechanism must be present to allow users to properly request access to the resources they need. The requests must always be reviewed and approved by user's management in addition to the business unit representing the owner of the assets being accessed. This will ensure that all access granted is properly requested, with an audit trail of how users managed to get that access. In any system that supports multiple roles, the users must always be encouraged and directed to request the least amount of privileges they need to perform their job. You will always face resistance from end users, as they would always like to have more privileges and access than they require. Therefore, this has to be assessed and verified carefully.

5. ACCESS REQUESTS REQUIREMENTS

There are a couple of things that must be considered as part of these access requests. Access must always be timed to a specific duration. Users must recertify and renew their access on a periodic basis if they need that access for a longer time. This helps to maintain a periodic access review cycle for all types of access granted to any user. It also ensures management and business units are aware of the access being granted to their users, as well as the responsibility and accountability that is applied to it.

In addition, access eligibility must be considered to minimize mistakes of granting access to users that do not actually need it as part of their job. For example, you should not have a help desk agent with the ability to request access to be a payroll administrator, because it is not expected to be performed as part of their job charter. Eligibility aids in maintaining a least privilege model for a company.

6. CONTINUOUS RECONCILIATION

This is definitely more important for organizations that have a very dynamic work environment where employees often rotate job roles. With regular rotations and job assignments, responsibilities will change. The main question to be raised here is "does the user need to inherit the access he/she had previously?" And many end-users will answer yes, but the correct answer is "it depends" on the nature of the old and new job responsibilities. Organizations struggle to find that linkage and distinction between needing or revoking old access. Therefore a safe approach must be considered here.

The safest approach is to revoke users' access and ask them to request again if needed. Therefore when a user moves from group A with responsibilities X, to group B with responsibility Y, we should immediately revoke all access they had as part of being in group A. Most probably they will not need that access completely, or at least partially, as it is expected they will be busy with new responsibilities. In addition, if they need that access, then their new manager needs to be aware and therefore approve any access being granted to users belonging to their group.

Continuous reconciliation is a fantastic concept, but it is not easy to be accomplished in practice. If you do not have the right tools to implement continuous reconciliation in the correct manner, then at minimum, there should be a process to notify all relevant account admins and system owners to ensure access of such users is appropriately revoked.

7. CONCLUSION

Identity and access management is a critical part of the cybersecurity posture of any company. Ensuring that it is implemented correctly is crucial. Regular assessment of IAM practices must be done on a regular basis, to ensure all related controls are intact and operating as expected. The IAM lifecycle consists of a Provisioning, De-Provisioning, Access Requests and Continuous Reconciliation. Keeping these elements in mind while deploying an IAM strategy in any company is very important.

REFERENCES

[1] Gartner_Inc. (n.d.). Definition of Identity and Access Management (IAM) - Gartner Information Technology Glossary. Retrieved September 14, 2020, from https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam

[2] Gamby, R. (2010, November 09). User provisioning best practices: Access recertification. Retrieved September 14, 2020, from https://searchsecurity.techtarget.com/tip/User-provisioning-best-practices-Access-recertification

[3] Curious about provisioning and deprovisioning? (n.d.). Retrieved September 14, 2020, from https://www.onelogin.com/learn/what-is-user-provisioning-and-deprovisioning