ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 10, Issue 3, pp: (5-7), Month: July - September 2022, Available at: www.researchpublish.com

Identity and Access Management (IAM) Processes and controls Automation

[1]Waleed A. Alamri, [2]Abdullah K. Almadani

Saudi Arabia

DOI: https://doi.org/10.5281/zenodo.6806491

Published Date: 07-July-2022

Abstract: **unauthorized access to critical IT systems accounts for up to 34% of all cyber attacks. Cyber attacks that aim to steal user data for monetary value, blackmailing or spying require gaining unauthorized access. Failing to revoke user privileged access is equivalent in risk as such users provides an entry point for hackers. One of the controls that can be implemented to protect organization from such risk is to develop an automated IAM process. IAM systems can be developed in-house or purchased as a ready solution from vendors.**

Keywords: **Automated access control, unauthorized access, CyberSecurity, Risk.**

I. INTRODUCTION

Identity Access Management (IAM) implementation is a crucial part in the cybersecurity world as it protects the information, resources, systems, and networks by ensuring that only the authenticated authorized users have access to the right resources at the right time. Unauthorized access is one of the major cybersecurity threats and the starting entry point of the adversary to compromise the targeted system or organization as 34% of all cyber attacks involve unauthorized access. Introducing and Implementing proper identity and access management (IAM) processes and controls can be achieved either automatically or manually. Manual application of access control can be challenging and inefficient especially in the large organization and will eventually result in unauthorized access. Every organization needs to develop a robust automated process to handle account and authorization lifecycle management. This paper illustrates the best practices of implementing automated IAM processes and controls.

II. BODY

A. Account and authorization lifecycle management

An account represents the identity of a user allowing the system to verify that the user is who he claims to be. However, an authorization defines the level of what each user can and cannot do after the authentication. As soon as an account/identity and role/authorization is created, the organization should start managing those accounts and roles using proper IAM controls to ensure that a user is only given the correct access level at the right time, as well as being revoked in a timely manner.

The account and authorization lifecycle management can be broken down into 4 phases:

- Provisioning: creating the account/role (objects), creating groups (group of users or roles), or granting and assigning the roles/groups appropriately

- Account access request review and approval: each account provisioning and roles assignment must be reviewed and approved by the already defined concerned people which could be: system owner, role/authorization owner, or user's management.

- Account and access recertification: the account and role should be created and granted for a specific period of time (already defined in the organization access policy and set in the target system) and revoked on a timely manner if it is not recertified.

- Account and access reconciliation: a process of matching each account or access with a valid approved access request to ensure the account and access was created and granted properly and prevent unauthorized access.

- De-provisioning: deleting the account/role (object), groups, or revoking and unassigning the roles if certain conditions have met.

All of the mentioned processes can be automated either by using and implementing off-the-shelf identity and access management (IAM) product or developing a custom platform, website, or scripts. Organizations planning to implement an access control system should consider three abstractions: access control policies, models, and mechanisms. Access control policies are high-level requirements that specify how access is managed and who may access information under what circumstances. For instance, policies may pertain to resource usage within or across organizational units or may be based on need-to-know, competence, authority, obligation, or conflict-of-interest factors. At a high level, access control policies are enforced through a mechanism that translates a user's access request, often in terms of a structure that a system provides. Access Control List is a familiar example. Access control models bridge the gap in abstraction between policy and mechanism. Rather than attempting to evaluate and analyse access control systems exclusively at the mechanism level, security models are usually written to describe the security properties of an access control system. Security models are formal presentations of the security policy enforced by the system, and are useful for proving theoretical limitations of a system.

B. automation of identity and access management processes and controls

Identity and access management processes and controls automation is essential in implementing IAM to overcome risks and threats, ensure the proper access is granted, prevent unauthorized access, keep track of all access requests, and enhance the customer experience. IAM automation can be achieved by:

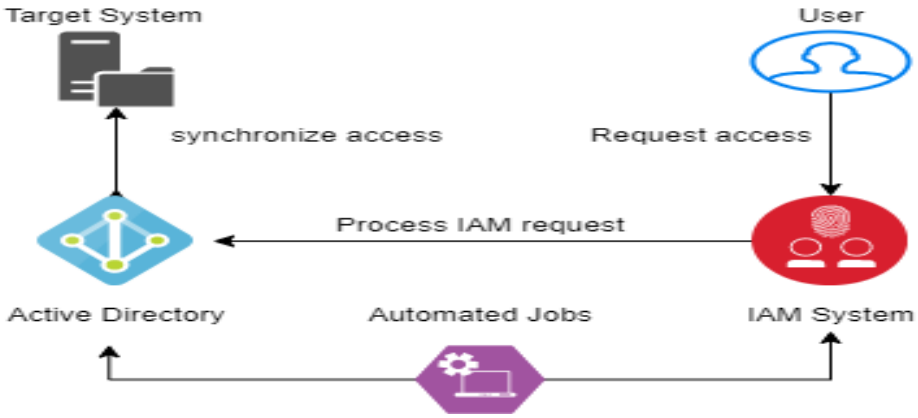
- off-the-shelf IAM platform

There are several solutions in the market to be used to centralize, unify, and streamline all access management controls in one system. Identity and access management (IAM) tools makes it easier for employees to securely access the data and applications they need to complete their duties. These solutions ensure that only authorized employees are accessing sensitive information. Such solutions come with many out-of-the-box connectors to be integrated with several systems or databases that introduce automated IAM processes, such as account and access provision, recertification, access request review, and de-provisioning. IAM tools' main benefits come from improving company security and increasing employee productivity. Many companies use IAM software to reduce the burden on their IT and security teams and eliminate human error as a result of manual access control processes while still ensuring that day-to-day business operations are not hindered. Each IAM system has pros and cons and the organization should define the requirements and business feasibility before implementing any of those solutions.

- In-house developed IAM solution, website, or system

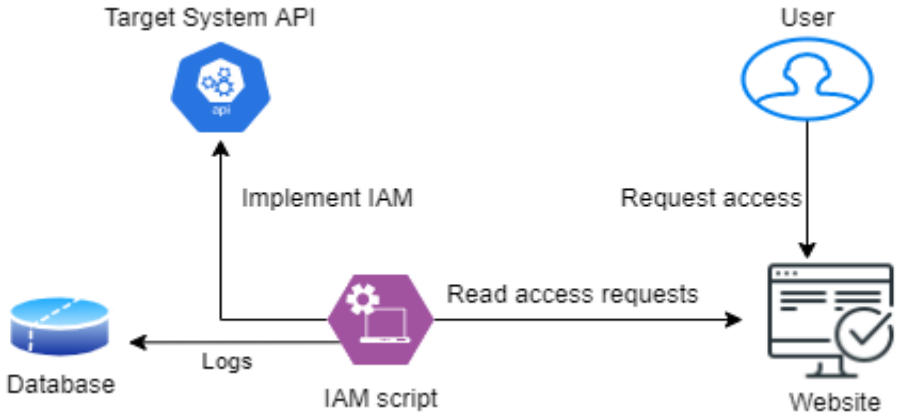
The organization can develop and automate its own IAM system by defining IAM policies, develop the IAM system to request account or roles/access, integrate it with all target systems they want to implement the controls on, keep audit logs for all processed events, and schedule automated jobs to check, verify, and action the account and access requests. After defining the IAM policies and standards, the organization should start to build and develop a centralized IAM system to handle and process users' access requests. The IAM system can depend on other system, groups, or objects (i.e. Active directory) to manage the accounts and maintain the authorization. Consequently, multiple integration should be implemented between either the IAM system or dependant system (i.e. AD) and the target system.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 10, Issue 3, pp: (5-7), Month: July - September 2022, Available at: www.researchpublish.com



- Simple IAM automation scripts

The organization can also develop automation simple scripts, such as python or PowerShell scripts, to automate IAM processes and controls. The script function is to connect to the target system directly through its API to perform IAM actions, but before doing so there must be a defined logic, procedure, and mechanism in the script to ensure the accuracy of the performed actions. The script also should be integrated with the data source (request access platform or website) to read all of the accounts and access requests in order to implement it. In addition, there should be a database or a log file to store all the actions and events. Several IAM processes can be implemented by a simple script: provisioning, de-provisioning, recertification, etc.



Furthermore, scripts can be stand-alone to automate specific IAM controls such as account and authorization recertification. a stand-alone script can also be used as a compliance and governance validation and verification (i.e. Cross check). To simplify a script connects to the system API, reads the access data and performs specific action and controls based on the organizations cybersecurity standards, policies, and the written logic.

III. CONCLUSION

In conclusion, for organizations to overcome the risk associated with manual implementation of access control proper automated IAM processes and controls must be implemented. Account and authorization lifecycle management must be taken in consideration when developing IAM process. IAM solutions can be either developed in house by the organization or purchased by specialized vendors in the field.

REFERENCES

[1] "Access Control Policy and Implementation Guides", Created September 02, 2016, Updated June 22, 2020, https://csrc.nist.gov/Projects/Access-Control-Policy-and-Implementation-Guides.

[2] BY JENN FULMER, "Best Identity Access Management (IAM) Solutions & Tools 2022", Created April 29, 2021. https://www.itbusinessedge.com/security/best-iam-software