УДК 351.9:347

Полонська О.К.

AUDITING AND MONITORING ACCESS IN IAM SYSTEMS: ENSURING REGULATORY COMPLIANCE AND DETECTING ANOMALIES

Анотація

В умовах зростаючих кіберзагроз критично важливим є ефективний контроль доступу до корпоративних даних. У статті розглядаються підходи до впровадження безперервного моніторингу та здійснення регулярного аудиту в системах управління ідентифікацією та доступом. Особливу увагу приділено використанню механізмів аналізу поведінки користувачів для швидкої ідентифікації аномалій та оперативного реагування на потенційні інциденти. Також пропонуються шляхи гармонізації внутрішніх політик інформаційної безпеки з актуальними регуляторними стандартами, що дає змогу суттєво знизити ризики несанкціонованого доступу та уникнути додаткових фінансових втрат через штрафи.

Ключові слова: *аудит безпеки, моніторинг доступу, кібербезпека, виявлення аномалій, управління ідентифікацією.*

Abstract

In the face of growing cyber threats, effective access control to corporate data is critically important. The article discusses approaches to implementing continuous monitoring and regular auditing in identity and access management systems. Particular attention is paid to the use of user behavior analysis mechanisms for rapid identification of anomalies and prompt response to potential incidents. It also suggests ways to harmonize internal information security policies with current regulatory standards, which allows significantly reducing the risks of unauthorized access and avoiding additional financial losses due to fines.

Keywords*: security auditing, access monitoring, cybersecurity, Anomaly Detection, identity management.*

In the development of a new generation of gadgets and technologies, it is difficult not to notice how quickly people are increasingly skillfully using technology to control, manage and ensure stability in the virtual environment of ordinary users' lives on the network. Identity and Access Management (IAM) is a system of policies, processes and technologies that helps manage digital identities and regulate user access to various resources in an organization. The term appeared in the 1990s, although it became widespread much later. Its functions are as follows: managing access to applications, databases, networks and individual files, if it needs to be configured on behalf of the administrator, which is called 'Centralized Management'. Auditing and accounting means monitoring the necessary, that is, permitted processes that are directly related to access. Authentication is the verification of the person who should be allowed access if the information about the person entered in the databases by the administrator of the settings. Authorization when the previous stage confirms that the person is "real", then this stage consists of determining what actions the user can perform according to the privileges (rights) granted to him. [1]

For cybersecurity, this system provides secure access to company resources such as databases, email and applications. Secure access is ensured using a combination of protocols, encryption algorithms and policies. The protocols used are OAuth 2.0 and OpenID Connect, where the first option is an access delegation that allows the user to grant third-party applications limited access to their data without transferring credentials, and the second option is a layer on top of OAuth 2.0 that adds authentication functionality, allowing clients to verify the user's identity and obtain basic information about them [2]. Encryption algorithms are used, namely: TLS/SSL, which encrypts data transmitted between the client and the server, ensuring the confidentiality and integrity of the connection. Password encryption, which focuses on modern hashing algorithms (e.g., bcrypt, scrypt) – for secure storage of passwords that cannot be recovered in their original form. Policies such as the "Principle of Least Privilege", which grants users only those permissions that are necessary to perform their tasks, which minimizes the potential harm from compromised credentials, and "multi-factor authentication (MFA)", which requires confirmation of the user's identity by multiple methods. The final component of software and hardware

security in this concept are 3 utilities: account administration, role management and user activity monitoring.

And speaking of IAM auditing, here are a few principles that are important and required of the responsible person performing this audit in the system:

1. Vulnerability detection: Find weaknesses in the access control system that can be exploited by attackers.

2. Regulatory Compliance: Ensure that the company complies with legal requirements and industry standards (e.g. GDPR, HIPAA) for data protection and access management.

3. Configuration Validation: Ensure that access rights are assigned correctly and comply with the principle of least privilege.

4. Activity Monitoring: Track and analyze user actions to detect suspicious or unauthorized behavior.

5. Process Optimization: Provide recommendations for improving identity and access management processes.

Let us move on to the very principle of operation of this important security system. Ensuring secure access to corporate resources involves two steps: identity management and access management.

Identity management: A login attempt is checked against a database that continuously records data about users with appropriate permissions. This data must be constantly updated due to employee turnover, changing roles and projects, and organizational scaling. Information recorded in the identity management database includes user names, job titles, manager or subordinate information, mobile phone numbers, and email addresses. Matching an employee's login information, such as username and password, with the identity information in the database is called authentication. Additional protections include: multi-factor authentication (a type of two-factor authentication) actor) – this requires only a mobile phone number, a gadget that directly reproduces the functionality of this number, or the user's email address. Access control is the second stage of IAM. In the first stage, IAM authenticates the identity of the user attempting to access, and in the second stage, it tracks the resources to which the user has permission. Most organizations provide different levels of access to resources and data, determined by factors such as position, length of service, security level, and project type [3]. Compliance with legal documents:

GDPR (General Data Protection Regulation) is a European Union Regulation that establishes rules for the processing and protection of personal data of EU citizens. Its purpose is to protect personal data, ensure citizens' rights to privacy, and manage the risks associated with this data. It applies to any organization that collects, stores, or processes personal data of EU residents. The only requirement is to obtain the user's consent to process the data, provide a privacy policy, and ensure data security.

ISO 27001 is an international standard that specifies requirements for establishing and maintaining an Information Security Management System (ISMS). Objective: to ensure the protection of a company's information assets, including the confidentiality, integrity and availability of data. Applies to any organization, regardless of size or type. Single Requirement: to identify and assess information security risks, implement appropriate controls and continually improve the security management system.

ISO 27001 compliance can help companies meet the requirements of the GDPR, as both standards are aimed at protecting information. ISO 27001 certification proves that a company has an effective information security management system, which strengthens the trust of customers and partners. [4]

GDPR, ISO 27001 and IAM (Identity and Access Management) are closely linked, as ISO 27001 provides the framework for establishing an Information Security Management System (ISMS) that encompasses IAM processes, while GDPR sets requirements for the protection of personal data that require strict access controls, such as through IAM. IAM is a key mechanism for complying with both standards, ensuring compliance with security policies, data access, role-based access control and auditing of user actions. [5]

Regarding the use and overall implementation of this system. Most organizations already have a basic identity management system in place, whether they recognize it as such or not. For example, Lightweight Directory Access Control (LDAP) or Active Directory can provide centralized user and password management. However, these solutions often lack the comprehensive functionality of an identity and access management system [2]. Regarding the financial plan, such a system is not

completely free, but there are free plans for basic needs (for example, up to 20 users in certain cloud versions). The cost is of course affected by the functionality, number of users, type of services and scale of the system itself. The main ways to use this system by students can be: creating different types of users (variety of roles or privileges for a specific person); applying JSON access policies (read-only for example); simulating scenarios from the smallest to the largest 'highest' privileges for the user, that is, in other words, the development of rights; CloudTrail log analysis (viewing log files) – a place where there is a record of successful and unsuccessful request attempts from specific users; simulating intentional denial of access (using restrictive policies) and attempting to perform prohibited actions.

REFERENCES

1. What is IAM? CircleCI. URL: https://circleci.com/ru/topics/identity-access-management-iam/#:~:text=Управление%20идентификацией%20и%20доступом%20(IAM, access%20k%20resursam%20vnoutery%20sistemy. (access date: 03.11.2025).
2. What is Identity and Access Management?. ISSP Training. URL: https://www.issp.training/post/shcho-take-keruvannya-identyfikatsiyeyu-ta-dostupom (access date: 03.11.2025).
3. What is an identity and access management system? | Microsoft Security Complex. Your request has been blocked. This could be due to several reasons. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-identity-access-management-iam (access date: 03.11.2025).
4. GDPR requirements and ISO 27001 standard. SIM-Networks – Dedicated Servers, Cloud Servers, VPS for Business. Your Goals, our Tech. URL: https://www.sim-networks.com/ukr/blog/gdpr-requirements-and-iso-27001-standard#:~:text=Certification%20according%20to%20ISO%2027001,number%20of%20legislative%20acts,%20in particular%20GDPR . (access date: 03.11.2025).
5. Obtaining ISO 27001 Certification for information technology. MILITARY LAWYER - LEGAL ASSISTANCE FOR MILITARY SERVICEMEN. URL: https://inseinin.com.ua/tpost/6u8k0ho361-otrimannya-sertifkats-iso-27001-nformats#:~:text=What%20is%20ISO%2027001?,development%20of%20measures%20to%20minimize%20them . (date of application: 03.11.2025).

Полонська Олена – курсант, Інститут спеціального зв'язку та захисту інформації, Національний Технічний Університет України "Київський політехнічний інститут ім. Ігоря Сікорського", м. Київ, c049smarttab@gmail.com

– cadet, Institute of Special Communications and Information Protection, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, c049smarttab@gmail.com