Кухар О. О., магістрант,
Россінський Ю. М., к.т.н., доцент,
Державний університет «Житомирська політехніка»

ПЕРЕВАГИ ТА ВИКЛИКИ АВТЕНТИФІКАЦІЇ У ГІБРИДНІЙ ІНФРАСТРУКТУРІ

Гібридні інфраструктури стають дедалі популярнішими серед сучасних компаній завдяки їхній здатності поєднувати сильні сторони хмарних і локальних рішень. Одним із ключових завдань таких систем є забезпечення надійної автентифікації й авторизації користувачів. Концепція hybrid identity, яка об'єднує локальні (on-premises) системи, такі як Active Directory (AD), і хмарні платформи, зокрема Azure Active Directory (AAD), виступає важливим елементом управління доступом у гібридному середовищі.

Основні переваги автентифікації у гібридних інфраструктурах:

- Централізоване управління ідентичностями. Організації можуть об'єднувати локальні та хмарні ресурси, спрощуючи адміністрування доступу. Це знижує ризик помилок, зменшує дублювання інформації та підвищує загальну ефективність управління ідентичностями.
- Гнучкість і адаптивність. Гібридна модель дозволяє організаціям забезпечувати мобільний доступ до ресурсів через хмарні технології, зберігаючи контроль над конфіденційними даними, що залишаються на локальних серверах.
- Сумісність із сучасними протоколами безпеки. Хмарні сервіси, наприклад AAD, підтримують такі стандарти, як OpenID Connect, OAuth 2.0 і SAML. Це забезпечує інтеграцію з багатьма додатками й сервісами.

Основні виклики автентифікації у гібридних інфраструктурах:

- Залежність від постачальників хмарних послуг. Необхідність довіряти постачальникам хмарних рішень створює ризики, пов’язані з витоками даних або можливими збоями системи.
- Складнощі інтеграції. Відмінності в архітектурі, протоколах і механізмах безпеки між локальними та хмарними платформами можуть ускладнити їхнє поєднання.
- Висока вартість підтримки. Синхронізація локальних серверів і хмарних платформ вимагає значних фінансових і технічних ресурсів, включаючи впровадження політик безпеки, забезпечення резервного копіювання та оновлення систем.

Рекомендації для оптимізації автентифікації:

- Впровадження багатофакторної автентифікації (MFA). MFA підвищує захист систем, забезпечуючи додатковий бар’єр для несанкціонованого доступу.
- Постійний моніторинг безпеки. Застосування інструментів для аналізу даних про автентифікацію, як-от Microsoft Sentinel, допомагає виявляти та попереджати потенційні загрози.
- Навчання співробітників. Організації повинні підвищувати обізнаність працівників про методи соціальної інженерії та правила захисту доступу.
- Автоматизація синхронізації облікових записів. Рішення, такі як Azure AD Connect, дають змогу автоматизувати синхронізацію даних між локальними та хмарними системами.

Отже, Hybrid identity є критично важливою для автентифікації у гібридній інфраструктурі, оскільки вона поєднує сильні сторони хмарних і локальних рішень. Для забезпечення високого рівня безпеки та ефективності необхідно інвестувати в сучасні технології, регулярне навчання персоналу та моніторинг систем.

Список використаних джерел

1. McCoy, D. R. (2016). Identity and Access Management: A Critical Component of Cybersecurity. URL: https://www.researchgate.net/publication/305471256_Fitting_logistic_multilevel_models_with_crossed_random_effects_via_Bayesian_Integrated_Nested_Laplace_Approximations_a_simulation_study

2. Oliveira, C. M. D., & Lima, R. H. M. C. S. (2020). A Study on Identity Management in Cloud Computing Environments. URL: https://medium.com/@oswaldo.dev.oliveira/comprehensive-guide-to-iam-on-aws-managing-identity-and-access-9e30ac10a22c.