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

РЕКОМЕНДАЦІЇ ДЛЯ ВДОСКОНАЛЕННЯ HYBRID IDENTITY У ГІБРИДНИХ IT-ІНФРАСТРУКТУРАХ

Гібридна ідентичність (hybrid identity) відіграє ключову роль у сучасних IT-середовищах, які поєднують локальні та хмарні сервіси. Її впровадження дозволяє організаціям зберігати контроль над конфіденційною інформацією, розміщеною на внутрішніх серверах, та одночасно користуватися перевагами хмарних технологій, такими як гнучкість, масштабованість і зручність доступу. Проте її ефективність залежить від належного налаштування, забезпечення безпеки та адаптації до сучасних вимог.

Проблеми, які виникають під час впровадження hybrid identity:

- Проблеми синхронізації облікових записів

Через відмінності у роботі систем автентифікації часто виникають затримки в оновленні прав доступу.

- Загрози кібербезпеці

Неправильно налаштована гібридна ідентичність може стати вразливим місцем для атак, таких як викрадення облікових даних чи фішинг.

- Залежність від інтеграційних рішень

Системи на кшталт Azure AD Connect вимагають постійного технічного обслуговування та оновлень для забезпечення надійності та відповідності сучасним стандартам безпеки.

Рекомендації для підвищення ефективності hybrid identity:

- Запровадження багатофакторної автентифікації (MFA). Додавання додаткового рівня перевірки, наприклад через мобільний додаток чи біометричні дані, суттєво знижує ризик компрометації облікових записів навіть за умови злому пароля.
- Інтеграція сучасних протоколів безпеки. Використання OpenID Connect, OAuth 2.0 або інших сучасних стандартів підвищує сумісність систем і забезпечує безпечний доступ до ресурсів.
- Регулярний моніторинг і аудит дій користувачів. Використання рішень, як-от Microsoft Sentinel, дозволяє відстежувати підозрілу активність у режимі реального часу та своєчасно реагувати на загрози.
- Автоматизація процесів управління ідентичностями. Рішення на кшталт Azure AD Identity Governance оптимізують створення, оновлення та видалення облікових записів, що особливо актуально для організацій із великою кількістю співробітників.
- Навчання співробітників основам кібербезпеки. Інформування персоналу про ризики, пов’язані з фішингом та іншими видами атак, допомагає значно знизити рівень загроз через людський фактор.
- Впровадження принципу Zero Trust. Цей підхід ґрунтується на тому, що кожен доступ перевіряється, незалежно від того, чи запит надходить із внутрішньої чи зовнішньої мережі. Інтеграція Zero Trust у гібридну ідентичність забезпечує додатковий рівень захисту

Приклади успішного впровадження:

- У міжнародній фінансовій компанії впровадження Azure AD і багатофакторної автентифікації сприяло зменшенню випадків компрометації облікових записів на 30%.
- Один із університетів інтегрував локальну Active Directory із платформою для дистанційного навчання через AAD, забезпечивши студентам безпечний доступ до освітніх матеріалів із будь-якого пристрою.

Отже, оптимізація hybrid identity дозволяє зменшити адміністративні витрати, підвищити рівень безпеки та забезпечити зручність користувачів. Впровадження багатофакторної автентифікації, моніторингу активності та сучасних протоколів сприяє захисту даних і запобіганню кіберзагрозам.

Список використаних джерел

1. Bayram, S. & Anwar, A. (2018). Hybrid Identity Management Systems: Challenges and Solutions URL: https://toxigon.com/hybrid-identity-management-guide.

2. Microsoft. (2021). Best Practices for Securing Azure Active Directory. URL: https://learn.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices