Секція 1

РОЗРОБКА СИСТЕМИ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ДЛЯ КОРПОРАТИВНОЇ МЕРЕЖІ

Мищенко М. О.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Піскачов О. І.

Актуальність. Сучасні корпоративні мережі часто стають мішенню для кібератак, які можуть завдати значних збитків як фінансових, так і репутаційних. Одним із найбільш ефективних методів захисту від несанкціонованого доступу є багатофакторна автентифікація (MFA), яка використовує декілька незалежних методів перевірки автентичності користувача [1]. Використання лише одного факту автентифікації, як от пароля, є недостатньо надійним у сучасних умовах. Впровадження MFA знижує ризик зловживання обліковими записами та забезпечує більш високий рівень безпеки корпоративних даних.

Мета. Ця доповідь присвячена дослідженню та розробці системи MFA для посилення захисту корпоративної мережі. Розглянуто сучасні методи MFA, їхню ефективність проти кібератак та практичні аспекти впровадження в корпоративному середовищі. Зосереджено увагу на аналізі загроз, виборі оптимальних методів автентифікації та рекомендаціях щодо інтеграції MFA з мінімізацією впливу на зручність користування для працівників.

Основні положення. MFA визначається як метод автентифікації, що використовує два або більше незалежних факторів для підтвердження особи користувача [2]. Ці фактори можуть включати те, що користувач знає (наприклад, пароль або PIN-код), те, що користувач має (наприклад, смартфон, токен, смарт-картку) та те, що користувач є (біометричні дані, такі як відбитки пальців або розпізнавання обличчя). MFA має ряд переваг, серед яких підвищений рівень безпеки, оскільки додаткові фактори значно ускладнюють несанкціонований доступ; захист від фішингу, оскільки навіть якщо зловмисник отримає пароль користувача, інші фактори залишаться недоступними; і відповідність регулятивним вимогам, адже багато галузей вимагають впровадження MFA для дотримання стандартів безпеки. Етапи впровадження системи MFA включають аналіз поточної інфраструктури, вибір оптимальних методів автентифікації для користувачів компанії, інтеграцію з існуючими системами управління доступом, навчання персоналу принципам роботи

MFA та постійний моніторинг ефективності системи [3]. Для успішного впровадження MFA потрібно налаштувати зручні методи автентифікації для мінімізації незручностей для користувачів, забезпечити технічну підтримку та резервні методи автентифікації, а також обережно поводитися з біометричними даними та іншою чутливою інформацією.

Висновок. Розробка та впровадження систем багатофакторної автентифікації є критично важливим кроком для забезпечення безпеки корпоративної мережі. Використання декількох факторів автентифікації значно знижує ризики, пов'язані з компрометацією облікових записів та несанкціонованим доступом до конфіденційної інформації. Хоча процес впровадження може бути складним і вимагати значних ресурсів, переваги, що надає така система, роблять її необхідною для сучасних підприємств. Постійний моніторинг, навчання користувачів та оновлення системи є ключовими аспектами для підтримки високого рівня безпеки у довгостроковій перспективі.

Список літератури

1. Сердюков Д. В., Сидоренко З. В. Багатофакторна автентифікація користувачів мобільних пристроїв у корпоративних мережах. URL: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/865b80bc-9adb-437c-9f29-05afa55ee869/content (дата звернення: 02.09.2024).
2. Впровадження систем багатофакторної аутентифікації. *TechExpert IT Company*. URL: https://techexpert.ua/implementation-of-mfa-systems (дата звернення: 04.09.2024).
3. Організація двофакторної автентифікації для сервера OpenVPN. *TechExpert IT Company*. URL: https://techexpert.ua/2fa-for-open-vpn-server (дата звернення: 04.09.24).

Відомості про авторів

Мищенко Максим Олександрович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», m.myshchenko@student.csn.khai.edu
Піскачов Олександр Іванович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., с.н.с., a.piskachev@csn.khai.edu