УДК 004.7

Томчук М. А.
Кальніченко Р. В.
Малініч П. П.

Покращення безпеки віртуальних мереж з двофакторним захистом

Вінницький національний технічний університет

Анотація
У цій публікації приділяється увага важливості та перевагам використання двофакторного захисту для безпеки віртуальних мереж. Розглядаються загрози для віртуальних мереж у цифровому світі, пояснюється концепція двофакторної аутентифікації та методи її впровадження. Наводяться приклади компаній, що успішно використовують двофакторний захист, та їхній вплив на безпеку мереж. Закликається до подальшого дослідження та вдосконалення систем захисту для забезпечення надійності віртуальних мереж у майбутньому.

Ключові слова: безпека, віртуальні мережі, двофакторний захист, аутентифікація, кіберзахист, технології безпеки, захист даних, інформаційна безпека, традиційні методи безпеки, кіберзлочинність.

Abstract
This thesis shows the importance and advantages of implementing two-factor protection for the security of virtual networks. It examines the threats faced by virtual networks in the digital world, explains the concept of two-factor authentication, and explores methods for its implementation. Real-world examples of companies successfully utilizing two-factor protection and their impact on network security are provided. The article concludes by calling for further research and improvement of security systems to ensure the reliability of virtual networks in the future.

Keywords: security, virtual networks, two-factor authentication, authentication, cybersecurity, security technologies, data protection, information security, traditional security methods, cybercrime.

Вступ

У сучасному цифровому світі, де віртуальні мережі стають основою для зв'язку, спільної роботи та передачі даних, безпека стає надзвичайно важливою. Віртуальні мережі є основою для бізнесу, освіти, медицини та багатьох інших сфер життя, тому захист їх даних та інфраструктури є пріоритетом для забезпечення нормального функціонування сучасного суспільства. Серед віртуальних мереж варто виділити два їх різновиди, де забезпечення безпеки є найбільш критичним: хмарні VPC та VPN [1].

З загальним збільшенням вживання віртуальних мереж зростає й потенційна кількість загроз для їх безпеки. Хакерські атаки, кіберзлочинність, витік даних та інші форми кіберзагроз стають все більш вишколеними та складними. Незахищені віртуальні мережі можуть стати легкою мішенню для зловмисників, що може призвести до серйозних наслідків для організацій та особистостей.

У зв'язку з цим виникає потреба у вдосконаленні заходів захисту для віртуальних мереж. Традиційних методів захисту, таких як використання слабких паролів або простих методів аутентифікації, вже не вистачає для ефективного протистояння сучасним кіберзагрозам. Запровадження новітніх технологій та інноваційних підходів до захисту може допомогти зменшити ризики та забезпечити відповідний рівень безпеки для віртуальних мереж.

Традиційні методи забезпечення безпеки доступу до віртуальних мереж

Серед традиційних методів забезпечення безпеки доступу до ВМ можна виділити три основних: парольний контроль доступу, обмеження фаєрволу та шифрування [2]. Самим елементарним методом захисту доступу до мереж є одним із найпоширеніших методів аутентифікації, що вимагаються для доступу до систем, додатків чи ресурсів в мережі. Вони можуть бути простими (легкими до вгадування) або складними (з використанням комбінацій букв, цифр та символів), і їх безпека залежить від їх складності та унікальності. Інший метод передбачає використання фаєрволів (мережевих екранів). Фаєрволи встановлюються на границі мережі для контролю трафіку, що входить та виходить з мережі [3]. Вони можуть блокувати небезпечний трафік, захищаючи мережу від зловмисників та шкідливих програм. Іншим дієвим методом захисту є шифрування. Але це використовується для захисту конфіденційності даних шляхом перетворення їх у незрозумілий для людини код. Шифрування може

застосовуватися як до даних під час їх передачі через мережу, так і до даних, що зберігаються на пристроях або серверах.

Традиційні методи безпеки мають свої переваги, проте вони також мають свої обмеження. Наприклад, слабкі паролі можуть бути легко скомпрометовані, а фаєрволи можуть не завжди ефективно виявляти та блокувати нові види загроз [4]. Також, аутентифікація за допомогою паролів може стати жертвою атак соціальної інженерії, коли користувачі введуть свої дані на фішингових сайтах. Двофакторна аутентифікація вимагає введення двох незалежних факторів ідентифікації, таких як пароль та одноразовий код, що надсилається на мобільний телефон. Цей метод підвищує безпеку, оскільки навіть якщо зловмисник дізнається пароль, він не зможе отримати доступ без другого фактора [5].

Впровадження двофакторного захисту

Двофакторна аутентифікація – це метод захисту, який вимагає від користувача подання двох незалежних факторів ідентифікації для підтвердження своєї особи перед отриманням доступу до системи, додатку чи ресурсу. Це включає в себе не лише традиційний пароль або PIN-код, а також щось унікальне саме для користувача, таке як одноразовий код, відбиток пальця, голосове впізнавання чи фізичний токен. Станом на сьогодні використання двофакторної аутентифікації стало базовою нормою забезпечення кібербезпеки. По-перше, це значно підвищує рівень безпеки, оскільки навіть якщо зловмисник дізнається пароль чи PIN-код, він все одно не матиме доступу до системи без додаткового фактора ідентифікації [6]. Це ускладнює можливість несанкціонованого доступу та зменшує ризик компрометації даних.

Для впровадження двофакторного захисту в віртуальних мережах існують різноманітні методи: SMS або E-mail коди, мобільні додатки для аутентифікації, фізичні токени та біометричні дані. У першому випадку користувач отримує одноразовий код або посилання на підтвердження доступу через SMS або електронну пошту. Цей код потрібно ввести разом з основним паролем для завершення процесу аутентифікації. Користувачі також можуть використовувати спеціальні мобільні додатки для отримання одноразових кодів або затвердження запитів на доступ. Є також токени – фізичні пристрої, які генерують одноразові коди або використовують технології близького зв'язку, такі як NFC або RFID, для підтвердження ідентифікації користувача. Крім них можливе використання унікальних біометричних даних, таких як відбиток пальця, розпізнавання обличчя, голосове впізнавання тощо, для підтвердження особи користувача.

Подальші перспективи

Вдосконалення захисту за допомогою двофакторного методу має великий потенціал і низку переваг, які варто розглянути для майбутнього розвитку сфери кібербезпеки:

- Збільшення стійкості до атак: двофакторний захист ускладнює завдання зловмисників, навіть у випадку, коли вони дізнаються основний пароль або PIN-код. Це допомагає попередити втрату конфіденційної інформації та недозволений доступ до систем.
- Зниження ризику фішингу та соціальної інженерії: двофакторна аутентифікація може допомогти уникнути атак, які базуються на обмані користувачів, оскільки навіть якщо зловмисник вдасться дізнатися основний пароль, він не зможе отримати доступ без додаткового фактора ідентифікації.
- Покращення відповідності до регуляторних вимог: багато регуляторних організацій та стандартів безпеки вимагають використання двофакторної аутентифікації для захисту конфіденційної інформації та особистих даних. Вдосконалення цих систем може допомогти підприємствам відповідати цим вимогам.
- Розвиток біометричних технологій: із зростанням популярності біометричних методів ідентифікації, таких як відбитки пальців, розпізнавання обличчя та голосу, двофакторна аутентифікація може стати ще надійнішою та зручнішою для користувачів.
- Дослідження нових методів аутентифікації: подальше дослідження та впровадження інноваційних методів аутентифікації, таких як шифрування на рівні апаратури та блокчейн-технології, можуть допомогти розвивати двофакторний захист у майбутньому [7].

Висновки

Впровадження двофакторного захисту є ключовим етапом у покращенні безпеки віртуальних мереж. Цей метод дозволяє ефективно захищати мережі від різних кіберзагроз, забезпечуючи високий рівень

безпеки для даних та інформації. Реальні приклади підтверджують успішність використання двофакторного захисту в різних компаніях і організаціях. Однак важливо продовжувати дослідження та вдосконалення цих систем для забезпечення стійкості та надійності віртуальних мереж у майбутньому. Тільки шляхом постійного удосконалення заходів безпеки можливо забезпечити безпеку та приватність у цифровому середовищі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Williams, D. (2017). "Introduction to Network Security Technologies." Boston: Pearson Education.
2. Taylor, R., & Clark, E. (2015). "Cybersecurity: Principles and Practices." New York: Cambridge University Press.
3. Малініч П. П. Актуальні проблеми кіберзахищеності систем центрального входу у багатосайтових освітніх інформаційних системах [Текст] / П. П. Малініч, О. О. Коваленко, І. П. Малініч // Матеріали міжнародної науково-технічної конференції «Сучасні тенденції розвитку техніки та технологій - 2023», Харків, 31 жовтня 2023. – 2023. – С. 10.
4. Johnson, A., & Brown, C. (2016). "Implementing Two-Factor Protection in Virtual Networks: Case Studies and Best Practices." Proceedings of the International Conference on Network Security, 78-89.
5. Малініч П. П. Впровадження технологій централізованої ідентифікації, автентифікації та авторизації користувачів у освітніх інформаційних системах [Текст] / П. П. Малініч, О. О. Коваленко, І. П. Малініч // Матеріали XVI міжнародної науково-практичної конференції «Інформаційні технології і автоматизація - 2023», Одеса, 19 – 20 жовтня 2023. – 2023. – С. 177–179.
6. Smith, J. (2014). "Enhancing Virtual Network Security with Two-Factor Authentication." Journal of Cybersecurity, 12(3), 45-56.
7. Баришев Ю. В. Метод автентифікації віддалених користувачів з прив'язкою до параметрів робочих станцій [Текст] / Ю. В. Баришев, О. П. Войтович // Тези доповідей учасників II Міжнародної науково-практичної конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації», Закарпатська область, Міжгірський район, село Верхнє Студене, туристичний комплекс «Едельвейс», 24-27 лютого 2016 р. - Київ : Видавництво Європейського університету, 2016. - С. 30-31.

Томчук Микола Антонович — канд. техн. наук, доцент кафедри Обчислювальної техніки, Вінницький національний технічний університет, e-mail: tomchuk@vntu.edu.ua
Кальніченко Роман Васильович — студент групи 1КІ-22мс, факультет Інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет
Малініч Павло Павлович — асистент кафедри Програмного забезпечення, Вінницький національний технічний університет

Mykola Tomchuk — Cand. Sc. (technologies), docent of the Computer Engineering department, Vinnytsia National Technical University, e-mail: tomchuk@vntu.edu.ua
Roman Kalnichenko — student of faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University
Pavlo Malinich — assistant lecturer of Software Development department, Vinnytsia National Technical University