УДК 004

Андрій ЛЕШКІВ, Людмила БАБАЛА

Західноукраїнський національний університет, м. Тернопіль, Україна

ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ ЯК ЗАСІБ ЗАХИСТУ ВІД ФІШИНГОВИХ АТАК

Вступ. Кібербезпека є однією з найбільш актуальних тем сучасного цифрового світу, адже зростання кількості кіберзагроз потребує новітніх та ефективних методів захисту. Одним із найбільш поширених видів атак є фішинг, що спрямований на отримання конфіденційної інформації користувачів шляхом обману. Враховуючи розвиток технологій, зловмисники застосовують усе складніші техніки для фішингових атак, що знижує ефективність традиційних методів захисту. У зв'язку з цим використання двофакторної автентифікації (2FA) стає важливим заходом захисту від кіберзагроз.

Мета: аналіз методів двофакторної автентифікації (2FA) як одного з найбільш ефективних способів захисту від фішингових атак, визначення його переваг, недоліків та можливих напрямів удосконалення.

1. Аналіз сучасних методів захисту від фішингових атак

Фішингові атаки, націлені на отримання конфіденційної інформації користувачів, залишаються серйозною проблемою у сфері кібербезпеки. За статистикою, близько 90% усіх порушень даних починаються з фішингових атак. Здебільшого, такі атаки здійснюються через електронну пошту або підроблені веб-сайти, які імітують легітимні ресурси. Фішери використовують різні техніки соціальної інженерії, щоб змусити користувачів надати свої паролі, номери кредитних карток, або інші конфіденційні дані.

Традиційні методи захисту від фішингу, такі як перевірка URL-адрес або фільтрація електронної пошти, мають обмеження. Наприклад, фішери можуть динамічно змінювати URL-адреси або створювати складні шаблони підроблених сторінок, які важко виявити звичайними методами [1]. Це дозволяє злочинцям залишатися непомітними та обходити багато сучасних систем безпеки.

Одним з найбільш ефективних методів підвищення безпеки є впровадження двофакторної автентифікації (2FA) (рисунок 1). 2FA є процесом підтвердження особи користувача за допомогою двох різних факторів: щось, що користувач знає (пароль) і щось, що користувач має (телефон, апаратний токен тощо).

Рисунок 1 - Приклад роботи двофакторної автентифікації

Такий підхід суттєво знижує ймовірність успішного здійснення атаки, навіть якщо пароль буде скомпрометовано.

Окрім 2FA, сучасні системи захисту включають такі технології, як:

- Machine Learning та AI-алгоритми: використання машинного навчання для виявлення аномалій в електронній пошті або на веб-сайтах може допомогти виявляти підозрілі дії та потенційні загрози.
- DMARC, SPF та DKIM: технології автентифікації електронної пошти, які допомагають знизити ризики фішингових атак, підвищуючи надійність відправника повідомлень.
- Фільтрація на основі репутації: деякі системи використовують бази даних репутації для оцінки легітимності URL-адрес або доменів на основі їхньої історії.

2. Двофакторна автентифікація як метод захисту від фішингових атак

2FA є важливим механізмом для підвищення рівня захисту користувачів, оскільки навіть у разі, якщо зловмисник отримає пароль, йому знадобиться доступ до другого фактору автентифікації. Ось більш детальний огляд трьох основних видів 2FA (таблиці 1):

1. SMS-код - користувач отримує одноразовий код на свій мобільний телефон у вигляді SMS. Цей метод є найбільш простим та зручним для кінцевих користувачів, тому що він не потребує встановлення додаткового програмного забезпечення. Проте, існують певні загрози, пов'язані з цим методом:
   - Вразливість до перехоплення повідомлень: зловмисники можуть використати атаки на сигнальні мережі (SS7) або методи соціальної інженерії, щоб отримати доступ до SMS.
   - Відновлення SIM-карти (SIM Swapping): є ризик того, що зловмисники можуть перенести номер телефону жертви на іншу SIM-карту [2].
2. Додаток-аутентифікатор - використання спеціального додатка, такого як Google Authenticator, Microsoft Authenticator або Authy, для генерації одноразових кодів. Цей метод має вищий рівень безпеки, ніж SMS-коди, оскільки код генерується локально на пристрої користувача і не передається через мережу:
   - Переваги: коди є менш вразливими до атак, оскільки вони генеруються на основі часу або лічильника, що зменшує можливість їх перехоплення.
   - Недоліки: для використання цього методу користувач повинен встановити додаткове програмне забезпечення та, у разі втрати пристрою, можуть виникнути труднощі з відновленням доступу.
3. Апаратний токен - фізичний пристрій, такий як YubiKey або Google Titan Security Key, що генерує одноразові коди або використовується для підтвердження автентифікації шляхом підключення до комп'ютера або смартфона через USB, NFC або Bluetooth. Цей метод вважається найбезпечнішим, оскільки апаратний токен практично неможливо підробити чи перехопити:
   - Сильні сторони: захищені від фішингових атак, оскільки токен використовує захищений канал для передачі даних і прив'язаний до конкретного сайту.
   - Слабкі сторони: апаратний токен може бути втрачений або забутий, що створює проблеми з доступом до акаунтів [3].

Таблиця 1 - Порівняння методів двофакторної автентифікації

Метод	Сильні сторони	Слабкі сторони
SMS-код	Простота використання	Вразливість до перехоплення повідомлень
Додаток-аутентифікатор	Висока надійність	Потребує встановлення додаткового додатку
Апаратний токен	Найвищий рівень захисту	Може бути втрачений або забутий користувачем

Двофакторна автентифікація допомагає значно знизити кількість успішних фішингових атак, оскільки навіть після компрометації пароля зловмиснику потрібно отримати доступ до другого фактору автентифікації, що є значно складнішим завданням. Дослідження показують, що 2FA здатна знизити кількість викрадених облікових записів на 50-80%, залежно від типу обраного методу [4].

Не зважаючи на численні переваги, 2FA також має свої недоліки:

- Зручність: для деяких користувачів установка додаткових додатків або носіння фізичних пристроїв може бути незручною.
- Технічні проблеми: в разі втрати доступу до другого фактору, відновлення може бути складним і вимагати додаткової верифікації особи.

Висновок. 2FA є ефективним засобом захисту від фішингових атак завдяки створенню додаткового бар'єру для кіберзлочинців. Попри деякі незручності для користувачів, такі як можливість втрати другого фактору, 2FA залишається одним із найефективніших методів забезпечення безпеки в цифровому середовищі. Подальші дослідження можуть бути спрямовані на інтеграцію новітніх технологій, таких як біометрична автентифікація, для створення ще надійніших рішень [5].

Перелік використаних джерел.

1. How to Protect Yourself Against a SIM Swap Attack, 2018. [Електронний ресурс]. - Режим доступу: https://www.wired.com/story/sim-swap-attack-defend-phone/

2. Keeper® Password Manager amp; Digital Vault - Authenticator App vs SMS Authentication: Which Is Safer?, 2024. [Електронний ресурс]. - Режим доступу: https://www.keepersecurity.com/blog/2024/02/15/authenticator-app-vs-sms-authentication-which-is-safer/

3. Blue Goat Cyber - Authenticator Apps vs. SMS for Two-Factor Authentication - Blue Goat Cyber, 2024. [Електронний ресурс]. - Режим доступу: https://bluegoatcyber.com/blog/authenticator-apps-vs-sms-for-two-factor-authentication-which-is-safer/

4. Okta Identity Solutions - What is SMS Authentication and Is It a Secure Solution?, 2024. [Електронний ресурс]. - Режим доступу: https://www.okta.com/blog/2020/10/sms-authentication/

5. InstaSafe - What Is SMS Authentication and Is It Secure? | Okta, 2024. [Електронний ресурс]. - Режим доступу: https://instasafe.com/blog/what-is-sms-authentication-and-is-it-a-secure-solution/