УДК 316.4

Д. А. Брухнов
А. О. Азарова

ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОЇ АВТОРИЗАЦІЇ НА ОСНОВІ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ЗІ ЗМІННИМ КЛЮЧЕМ ТА ЗАХИСТОМ ВІД BRUTE FORCE

Вінницький національний технічний університет

Анотація

У дослідженні вивчено різні методи захисту облікових записів на основі двофакторної аутентифікації засобами застосування змінного ключа та захистом від brute force. Вивчено етапи роботи алгоритму захисту від brute force та запропоновано відповідні рекомендації щодо підвищення рівня захищеності авторизації.

Ключові слова: двофакторна автентифікація, brute force, багатофакторна автентифікація, функції.

Abstract

Various methods of account protection based on two-factor authentication by means of variable key application and brute force protection have been studied. The stages of operation of the brute force protection algorithm are studied and the corresponding recommendations on increase of the level of authorization protection are offered.

Keywords: two-factor authentication, brute force, multifactor authentication, functions.

Вступ

Можливість несанкціонованого доступу до облікового запису вимагає створення додаткового рівня захисту на основі багатофакторної аутентифікації (MFA). Це метод аутентифікації (ідентифікації), що вимагає від користувача надання двох або більше доказів особистості, щоб отримати доступ і увійти у обліковий запис. І тільки після введення всієї цієї необхідної інформації можно отримати доступ до облікового запису. Це може бути номер телефону, адреса електронної пошти або відповідь на якесь секретне питання. Двофакторна аутентифікація (2FA) вимагає двічі підтвердити свою особу, тоді як багатофакторна – MFA – перевіряє особу за допомогою багатьох факторів, таких як біометричний, розпізнавання обличчя, час, місцезнаходження та ін. [1].

Разом із тим, доволі поширеним несанкціонованим видом доступу до облікового запису є підбір паролів для входу на веб-ресурс – Brute Force (*брутфорс* – пер. з англ. *груба сила*) атаки. Це метод підбору пароля, що полягає в пошуку пароля з безлічі всіх його можливих значень шляхом їх повного перебору. При цьому зазвичай враховується найменша і найбільша можлива довжина пароля [3].

Розглянемо різні фактори автентифікації:

- фактор знання. Інформація відома користувачеві: пароль, PIN-код, графічний ключ.
- фактор володіння. Пристрій, що належить користувачеві: смартфон, токен, апаратний ключ безпеки.
- Фактор властивості. Біологічні властивості, якими володіє користувач: відбиток пальця, малюнок сітківки ока, голос.

Робота алгоритму двофакторної аутентифікація 2FA полягає у виконанні двоетапного процесу перевірки:

Перший етап:

1. Сайт або програма пропонує вхід.
2. Вводиться інформація, що відома користувачеві: як правило, це ім’я користувача та пароль.
3. Після введення комбінації імені користувача та пароля сервер сайту знаходить і перевіряє особу.
4. Для процесів аутентифікації без пароля веб-сайт генерує унікальний ключ безпеки. Ключ безпеки обробляється постачальником послуг аутентифікації та перевіряється сервером веб-сайту.

Другий етап:

1. Потрібно ввести одноразовий код, згенерований на попередньому кроці, клацнути push-повідомлення, надане постачальником ідентифікаційних даних, або вставити універсальний маркер безпеки другого фактора (U2F), щоб підтвердити особу.

Виконавши обидва етапи автентифікації, користувач може отримати доступ до свого облікового запису [4].

Одним із можливих засобів захисту від brute force є блокування IP-адрес (Fail2Ban). Використовуючи регулярні вирази, Fail2Ban перевіряє файли журналів на різні помилки аутентифікації, шукає експлойти та інші записи, які можуть вважатися підозрілими. Ведеться підрахунок подібних записів журналу, і, коли їх кількість досягає певного значення, Fail2Ban

відправляє повідомлення електронною поштою або блокує IP-адресу зловмисника на певний період часу. Після закінчення періоду блокування IP-адреса автоматично розблоковується.

Логіку роботи Fail2Ban визначають Джейли. Джейла являє собою набір правил для конкретного сценарію. Налаштування Джейла визначають, що потрібно зробити в разі, якщо виявлена атака відповідно до визначеного фільтром (набором з одного або кількох регулярних виразів, що використовуються для моніторингу журналів) [5].

Функція блокування IP-адрес уможливлює:

- дозвіл на весь вхідний трафік з певного домену;
- захист від спуфинга за допомогою автоматичного налаштування діапазонів дозволених IP-адрес.

Блокування IP-адрес застосовується для доменів, у яких немає запису SPF або в яких використовуються сторонні додатки для відправки електронної пошти від імені домена.

Встановлення блокування IP-адрес виконується в три етапи:

- додавання домену;
- налаштування дозволеного діапазону IP-адрес;
- вибір дії і налаштування звіту про недоставку (NDR).

Слід зазначити, що проблем зі зломом через брутфорс можна уникнути, якщо:

- створювати довгий пароль з букв, цифр і спецсимволов;
- не використовувати в паролі особисту інформацію або будь-які елементи логіна;
- для всіх акаунтів створювати свої унікальні паролі;
- регулярно, приблизно один раз на місяць, змінювати паролі;
- на веб-сайтах захищати вхід від численних спроб введення даних.

Висновки

Отже, оскільки двофакторна аутентифікація (2FA) вимагає двічі підтвердити свою особу, то це один з можливих ефективних методів захисту облікового запису користувача. Слід пам’ятати, що інформаційна безпека, в першу чергу, знаходиться в руках користувача. Дотримуючись певних правил і використовуючи доступні рішення для захисту облікових даних, можна самостійно забезпечити високий рівень безпеки. Важливим фактором забезпечення захищеності інформації є своєчасне залучення новітніх інструментів і засобів безпеки. Не варто відкладати на майбутнє організацію безпеки – впровадження додаткового фактора захисту може запобігти негативним наслідкам і допоможе уникнути пов’язаних з ними збитків.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Що таке MFA — багатофакторна аутентифікація? URL : https://datami.ua/shho-take-mfa-bagatofaktorna-autentifikatsiya/ (дата звернення 7.03.21).
2. Захист сторінок логіна від brute force атак URL : https://ua.waykun.com/articles/zahist-storinok-logina-vid-brute-force-atak.php (дата звернення 7.03.21).
3. Что такое Brute force и как делать проверку на эту уязвимость с помощью программы Hydra+Burp Suite? https://svyat.tech/%D0%A7%D1%82%D0%BE-%D1%82%D0%B0%D0%BA%D0%BE%D0%B5-Brute-force-%D0%B8-%D0%BA%D0%B0%D0%BA-%D0%B4%D0%B5%D0%BB%D0%B0%D1%82%D1%8C-%D0%BF%D1%80%D0%BE%D0%B2%D0%B5%D1%80%D0%BA%D1%83-%D0%BD%D0%B0-%D1%8D%D1%82/ (дата звернення 7.03.21).
4 Sagar J. Two-Factor Authentication: A Valuable Addition to Account Security. URL : https://learn.g2.com/two-factor-authentication (дата звернення 7.03.21).
5. Защита от брутфорс-атак (Fail2Ban). URL : https://docs.plesk.com/ru-RU/obsidian/administrator-guide/%D0%B0%D0%B4%D0%BC%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D1%80%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80%D0%B0/%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B0-%D0%BE%D1%82-%D0%B1%D1%80%D1%83%D1%82%D1%84%D0%BE%D1%80%D1%81%D0%B0%D1%82%D0%B0%D0%BA-fail2ban.73381/ (дата звернення 7.03.21).
6. Как блокировать IP-адреса в Google Workspace. URL: https://support.google.com/a/answer/ 6047998?hl=ru (дата звернення 7.03.21).

Брухнов Даніїл Андрійович *– студент групи Уб-17б,факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: kariababienko03@gmail.com;*

Brukhnov Daniil *– student of the Ub-19b group, faculty of Management and Information Security, Vinnitsa National Technical University, Vinnitsa, e-mail: kariababienko03@gmail.com;*

Азарова Анжеліка Олексіївна – *к. т. н., професор каф. МБІС, заст. декана ФМІБ з наукової роботи та міжнародного співробітництва, Вінницький національний технічний університет, Вінниця.*

Azarova Anzhelika – *Candidate of technical sciences, Professor of the Department MBIS, Deputy dean of FMIS of research and international Cooperation., Vinnytsia National Technical University, Vinnytsia.*