УДК 004.056.3
Ревнюк О. – ст. гр. СБм-61
(Тернопільський національний технічний університет імені Івана Пулюя)

РОЗРОБКА СПЕЦІАЛІЗОВАНОЇ СИСТЕМИ КЕРУВАННЯ ПАРОЛЯМИ З МЕТОЮ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ ТА БЕЗПЕКИ ПІДПРИЄМСТВ

UDC 004.056.3
Revnuk O.

DEVELOPMENT OF A SPECIALIZED PASSWORD MANAGEMENT SYSTEM WITH THE PURPOSE OF IMPROVING THE EFFICIENCY OF ENTERPRISES'S FUNCTIONING AND SECURITY

Для нікого не є секретом те, що інтернет та цифрові технології стають невід'ємною частиною нашого життя. Пандемія COVID-19 лише прискорила темпи переходу у віртуальний простір. Сьогодні все від покупок до навчання, від виписки рецептів до перевірки документів, що посвідчують особу, відбувається в мобільних додатках або ж у веб-браузері. Це призвело до збільшення кількості користувачів електронних ресурсів і, як наслідок, збільшення кількості логінів та паролів необхідних для запам'ятовування. Велика кількість людей задля спрощення запам'ятовування використовують дуже слабкі паролі та повторюють їх на різних веб-сайтах. Дуже часто можна зіткнутись із ситуацією, де в паролі містяться різні асоціативні дані: дата народження, особисті дані, назва вулиці, кличка домашнього улюбленця тощо. Але найгіршими є випадки, в яких люди вводять один і той же пароль на різноманітних ресурсах. Адже, якщо хоча б один із цих облікових записів скомпрометований, то вже не має значення, наскільки надійним був пароль – хакери зможуть легко використовувати його, щоб потрапити в інші облікові записи. Основна причина використання однакових даних для входу – складність запам'ятовування різноманітних комбінацій.[1]

Менеджер паролів – безпечна, автоматизована та повністю цифрова заміна маленького блокнота з записами секретних даних для входу.[2] Основною задачею програмного забезпечення є безпечне керування даними для доступу в облікові записи. Окрім цього, наявність прогресивного генератора ключів, забезпечить використання сильного пароля для безлічі ресурсів. Проте, однією з типових загроз для такого виду програм є можливість викрадення бази даних зловмисниками. Великою проблемою в такому випадку стає зберігання паролів в базі даних у відкритому вигляді. Найкращий варіант виходу з цієї ситуації - використання криптографічних хеш-функцій. В такому випадку в базі даних зберігається не сам пароль, а його хеш. Щоразу при введенні паролю, система обчислює його хеш і порівнює зі збереженим хешом в базі даних. Цей підхід дозволяє безпечно використовувати паролі, проте у випадку, якщо людина забула пароль, то маючи хеш-функцію від паролю, не зможе його відновити. Двостороннє шифрування є одним з оптимальних підходів для вирішення проблеми безпечного зберігання паролів.[3] Зашифрувати пароль можливо двома шляхами:

1. Шифрування за допомогою ключа, що знаходиться в базі даних. Це метод стандартний та зручний для користувача. Тому що ключ для розшифрування вводити не потрібно.
2. Шифрування за допомогою особистого ключа. Безпечний метод.

Другий метод унеможливлює викрадення пароля. Адже, навіть викравши базу даних, зловмисник не зможе розшифрувати дані без ключа.

Існує багато стандартних програмних продуктів для організації безпечного зберігання паролів. Dashlane, Onesafe, LastPass та інші менеджери паролей, які мають зручний функціонал для зберігання даних. Правда, деякі з них часто нехтують правилами безпеки особистих даних. Будь яка людина, яка опиниться біля монітору з відкритою програмою, зможе побачити паролі користувача. Причиною того є те, що паролі виводяться з бази даних в відкритому вигляді.

Аналіз відомих програмних продуктів, які можна використовувати для зберігання паролів, показав, що, не зважаючи на незначні відмінності, програмні рішення є доволі стандартними і не пристосованими для потреб управління паролями бізнесу. Дослідження потреб бізнесу показало, що більшість існуючих організацій потребують менеджери паролів з можливістю розподілу ролей та доступів до інформації. Зокрема, працівники окремого відділу повинні мати доступ до спільної інформації.

Розробка програмного забезпечення, яке дає можливість не тільки розподіляти зашифровані паролі організації між користувачами – але й якісно захищати від впливу сторонніх чинників – основна ідея роботи. Система буде корисною, як для власного користування, так і для організацій. Користувач зможе зберігати доступи до ресурсів в трьох виглядах:

1. Особистому
2. Категорійному
3. Організаційному

Власник організації має можливість створювати підрозділи та здійснювати керування користувачами. Можливість визначення ролей працівників спростить систему управління бізнесом. Два методи шифрування забезпечують ще більш якісну систему захисту від зловмисників, а простота використання та відсутність перевантаженого функціоналу допоможе освоїтись в системі користувачам з різними навичками роботи з ПК.

Розробка менеджеру паролів, пристосованого до вимог бізнесу, покращить інформаційну безпеку організації та пришвидшить роботу працівників тих чи інших відділів.

Література.

1. Andrew C. C. Why You Need a Password Manager. Yes, You. [Електронний ресурс] / Cunningham Clifton Andrew // Wirecutter. – 2019. – Режим доступу до ресурсу: https://www.nytimes.com/wirecutter/blog/why-you-need-a-password-manager-yes-you/.
2. What is a password manager? [Електронний ресурс] – Режим доступу до ресурсу: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers.
3. 5 Benefits of using a password manager [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://blog.envisionitsolutions.com/5-benefits-of-using-a-password-manager.