Автор:
Магда Матвій Олексійович
студент 11 КНм групи
спеціальності 122 Комп'ютерні науки
Науковий керівник:
кандидат педагогічних наук,
старший викладач кафедри комп'ютерної та програмної інженерії
Галицький Олександр Вадимович

ПРОГРАМНА СИСТЕМА ДЛЯ МЕНЕДЖМЕНТУ СЕКРЕТНИХ ДАНИХ

Анотація: Останні роки загрози розкриття секретних даних для побутових і корпоративних користувачів тільки збільшуються. Насамперед це стосується облікових даних та ключів (паролів) до них, але й інші секретні дані під загрозою. Для комфортної адаптації у світі кібербезпеки необхідно інтегрувати рішення та інструменти для забезпечення безпеки секретних даних серед масового користувача.

Ключові слова:секрет, ключ, пароль, програма, менеджмент, кібербезпека.

Вступ. Рівні загроз у кібербезпеці еволюціонують із кожним днем. Так само і розвиваються відповідні до них заходи та інструменти з безпеки.

Однією з самих важливих проблем у кібербезпеці є нехтування правилами та рекомендаціями щодо створення, зберігання та управління критично важливими секретними даними, такими як: дані до облікових записів та їх паролі, ключі доступу до ресурсів, сертифікати валідації, файли ключів для віртуальних серверів та інші. Ця проблема є актуальною як в побутовому так і в корпоративному і урядовому сегментах. Її наслідками можуть бути втрати критично важливих даних, що може принести величезні збитки та безповоротну втрату даних.

Для часткового вирішення цієї проблеми достатньо дотримуватись простих рекомендацій. Для повного вирішення необхідно використовувати спеціально призначені для цього сервіси, так звані менеджери секретів.

Мета роботи полягає в наступному: створити програмну систему для створення, безпечного зберігання та керування обліковими даними.

Виклад основного матеріалу. Проблему створення, або ж іншими словами – генерації ключів або паролів можна частково вирішити мануальним способом, дотримуючись широковідомих рекомендацій щодо генерації ключів: використовувати як великі, так і маленькі літери, використовувати цифри, використовувати спеціальні символи та використовувати інакші ніж латинські літери, наприклад кирилицю. Також довжина ключа має бути достатньо великою. На сьогоднішній день 20 символів є достатнім рівнем для довжини паролю, якщо використовувати генерацію із достатньо високою ентропією, проте методи атак зловмисників еволюціонують із кожним днем, тому ця довжина постійно збільшується. Важливо відмітити, що сама по собі довжина не є об'єктивною характеристикою без ентропії. Пароль може бути довгим, проте у нього може бути маленький символьний алфавіт і низька ентропія – багато повторюваних, або послідовних символів. Також важливо створювати ключі, що не знаходяться у базі так званих «словників» паролів – популярні паролі, що можуть навіть бути складними, проте вончуєш а щи будуть перевірені одними із перших. Проте, навіть дотримання всіх цих правил не забезпечує стовідсоткову надійність згенерованому ключу, бо як на своєму досвіді показує соціальна інженерія – у багатьох випадках ключ, згенерований людиною можна відтворити, використовуючи методи соціальної інженерії. Якщо ж ключ буде генерувати програма за допомогою криптографічно-стійкого алгоритму – шанси його відтворити будуть близькими до нуля.

Навіть якщо проблема створення генерації ключів та інших секретних даних вирішена, проблема їх зберігання нікуди не зникає. Яким би надійним не був згенерований секрет – якщо недбало відноситися до його зберігання, він легко може бути отриманий зловмисниками. На сьогоднішній день самий надійний спосіб зберегти секрет – це запам'ятати його і ніколи нікому не повідомляти і ніде не записувати. Проте хоч цей спосіб і є самим надійним, він не дозволить навіть побутовому користувачу користуватися ним у повній мірі. По правилам кібербезпеки не можна використовувати один і той самий ключ або пароль у декількох місцях, бо при компрометації секрету в одному місці – він може бути використаний для доступу до іншого. Таким чином для кожного окремого місця завжди має бути унікальний ключ. Додаючи до цього ще й вищезазначені рекомендації з генерування ключів щодо їх довжини та різноманіття символів можна дійти до висновку що навіть середньостатистичному побутовому користувачу неможливо тримати своїй у пам'яті секрети, так як на сьогоднішній день кількість різноманітних сервісів якими люди користуються кожен день досить велика і тільки збільшується. Через це, навіть якщо ми маємо надійні ключі або паролі, ми маємо їх десь зберегти. Зазвичай люди записують їх на папері, або ж у нотатки на комп'ютері або телефоні, але очевидно, що це ненадійно, бо при отриманні зловмисником доступу до девайсу він отримає всі дані. Можна використовувати більш надійні сховища для критичних даних, наприклад зберігати їх у зашифрованому сховищі для розшифрування якого необхідно використовувати спеціальний ключ, який для найбільшої надійності користувач має запам'ятати і ніде не записувати.

Програмна система для менеджменту секретних даних об'єднує у собі генерування ключів, зберігання їх та інших секретних даних, а також дозволяє зберігати облікові дані та надає інструменти для керування. Такі програми часто називають менеджером паролів, менеджером ключів, або менеджером секретів.

Висновок. Для забезпечення безпеки своїх облікових даних необхідно використовувати рішення та інструменти для менеджменту секретними даними. Для інтегрування таких рішень у маси можна інтегрувати рішення у соціальні мережі, що дозволить побутовим користувачам простіше адаптуватися до них.

Список використаних джерел:

1. SafetyDetectives. The 20 Most Hacked Passwords in the World: Is Yours Here?.SafetyDetectives. URL: https://www.safetydetectives.com/blog/the-most-hacked-passwords-in-the-world/

2. Neumann A. The Integrated Information Environment / Alexander Neumann, 2021. – 45 с.