Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Аналіз витоків даних у великих організаціях та методи їх попередження

Виконав: студент 4 курсу, групи СБ-41
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

_____ *Бучко А.М.*
(підпис) (прізвище та ініціали)

Керівник _____ *Деркач М.В.*
(підпис) (прізвище та ініціали)

Нормоконтроль _____ *Лобур Т.Б.*
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ *Загородна Н.В.*
(підпис) (прізвище та ініціали)

Рецензент _____ _____
(підпис) (прізвище та ініціали)

Тернопіль
2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра Кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«____» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Бучко Анастасії Миколаївні
(прізвище, ім'я, по батькові)

1. Тема роботи Аналіз витоків даних у великих організаціях та методи їх попередження

Керівник роботи к.т.н., доц. Деркач М.В.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 04 » 04 2023 року № 4/7-349

2. Термін подання студентом завершеної роботи 16.06.2023

3. Вихідні дані до роботи наукові літературні джерела

4. Зміст роботи (перелік питань, які потрібно розробити)

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	Пилипець М.І., доцент кафедри МТ		

7. Дата видачі завдання 04.04.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	09.04 – 12.04	*Виконано*
2.	Підбір джерел про основні фактори і канали витоку інформації	14.04 – 17.04	*Виконано*
3.	Опрацювання джерел про основні фактори і канали витоку інформації	19.04 – 29.04	*Виконано*
4.	Розроблення автоматизованих запитів до пошукових систем	30.04 – 11.05	*Виконано*
5.	Тестування автоматизованих запитів до пошукових систем	12.05 – 20.05	*Виконано*
6.	Оформлення розділу «Аналіз витоку даних в організаціях»	20.05 – 23.05	*Виконано*
7.	Оформлення розділу «Методи запобігання витоку даних»	23.05 – 28.05	*Виконано*
8.	Оформлення розділу «Аналіз пошукових систем зламаних акаунтів»	28.05 – 05.06	*Виконано*
9.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи хорони праці»	05.06 – 07.06	*Виконано*
10.	Оформлення кваліфікаційної роботи	07.06 – 10.06	*Виконано*
11.	Нормоконтроль	11.06 – 13.06	*Виконано*
12.	Перевірка на плагіат	14.06 – 17.06	*Виконано*
13.	Захист кваліфікаційної роботи	20.06	

Студент _____ Бучко А.М.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Деркач М.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Аналіз витоків даних у великих організаціях та методи їх попередження // Кваліфікаційна робота освітнього рівня «Бакалавр» // Бучко Анастасія Миколаївна // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2023 // С. 56, рис. – 16 , табл. – 0, кресл. – 0, додат. – 1, бібліогр. – 12.

Ключові слова: ВИТІК ДАНИХ, АНАЛІЗ, КОРИСТУВАЧ, ВЕБ-ТРАФІК, ОРГАНІЗАЦІЯ, КОНФІДЕНЦІЙНІСТЬ.

У кваліфікаційній роботі було проведено ґрунтовне дослідження основних методів та причин витоку інформації з великих організацій. Були проаналізовані різноманітні способи запобігання таким витокам та розроблені ефективні інструменти для пошуку та аналізу цих витоків.

Один з ключових результатів цієї роботи - розробка інструменту з використанням мови програмування Python. Цей інструмент підключається до API провідних сервісів, таких як HIBP та Intelx, що дозволяє отримати доступ до великого обсягу даних про витоки інформації.

Застосування цього інструменту полягає у введенні домену сайту організації, яка потенційно може стати жертвою витоку даних. Інструмент автоматично виконує пошук та аналіз витоків даних, пов'язаних з цим доменом.

Крім того, було розроблено додатковий функціонал, який інтегрує пошук знайдених електронних адрес за допомогою телеграм бота PasswordSearchBot. Цей бот проводить пошук за відповідними електронними адресами, які пов'язані з доменом організації, що була об'єктом пошуку.

ANNOTATION

Analysis of data breaches in large organizations and methods of their prevention. // Buchko Anastasiia // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Cybersecurity Department, SB-41 group // Ternopil, 2023 // Pages – 56, figures – 16, tables – 0, sketches - 0, addendums - 1, references - 12.

Keywords: DATA BREACH, ANALYSIS, USER, WEB TRAFFIC, ORGANIZATION, PRIVACY.

In the qualification work, a thorough study of the main methods and reasons for leaking information from large organizations was conducted. Various ways to prevent such leaks have been analyzed and effective tools for finding and analyzing these leaks have been developed.

One of the key results of this work is the development of a tool using the Python programming language. This tool connects to the APIs of leading services such as HIBP and Intelx, allowing access to a large amount of data on leaks.

The application of this tool is to enter the website domain of an organization that could potentially become a victim of a data breach. The tool automatically searches and analyzes data leaks related to this domain.

In addition, an additional functionality was developed that integrates the search for found e-mail addresses using the Telegram bot PasswordSearchBot. This bot searches for relevant email addresses that are associated with the domain of the organization that was the object of the search.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

DLP - Data Loss Prevention

IAM - Identity and access management

UEBA - User and entity behavior analytics

ISMS - information security management systems

PDCA - Plan-Do-Check-Act

PII - personally identifiable information

ЗМІСТ

ВСТУП

Витік даних — це проблема, яка щодня набуває розголосу у всьому світі. Незалежно від того, чи йдеться про жахливе «вибачте, цей електронний лист призначався комусь іншому», чи втрачений USB-пристрій, чи зловмисний вчинок з боку незадоволеного співробітника, витік даних зростає.

Реальність така, що зараз є більше каналів для спілкування із зовнішньою аудиторією, отже, й більша ймовірність витоку даних або можливих порушень.

Стає очевидним, що витік даних може відбуватися через різні канали, такі як навмисні порушення, хакерство, внутрішні загрози, людські помилки або неадекватні заходи безпеки. Це підкреслює необхідність багатогранного підходу до запобігання витоку даних.

Впровадження класифікації даних і контролю доступу дозволяє організаціям ідентифікувати та обмежувати доступ до конфіденційних даних на основі їх рівня чутливості. Шифрування як у стані спокою, так і під час передачі додає додатковий рівень захисту, ускладнюючи неавторизованим особам розшифрувати дані, навіть якщо вони отримають доступ.

1. АНАЛІЗ ВИТОКУ ДАНИХ В ОРГАНІЗАЦІЯХ

1.1 Основні фактори і канали витоку інформації

Витік інформації, який також можна назвати малопомітною крадіжкою даних, передбачає несанкціоновану передачу електронних або фізичних даних від організації зовнішнім одержувачам або адресатам. Зловмисники часто крадуть дані за допомогою облікових записів електронної пошти або Інтернету. Вони також можуть використовувати мобільні пристрої зберігання даних, такі як USB-ключі, ноутбуки та оптичні носії.

Витік інформації може бути наслідком цілеспрямованих внутрішніх дій, спрямованих на завдання шкоди організації, або як частина більшої схеми шахрайства з банківськими платежами. Кіберзлочинці шукають різну інформацію у витоках даних, зокрема інформацію про клієнтів і комерційну таємницю. Обсяг і тип витоку визначає шкоду, завдану організації. Саме тому важливо ознайомитись з найбільш поширеними факторами витоку інформації.

Можливі канали витоку інформації поділяються на чотири групи.

1-а група – складається з каналів, які стосуються доступу до компонентів системи обробки даних без необхідності будь-яких модифікацій цих компонентів.

До цієї групи входять канали:

— дистанційне негласне відеоспостереження або фотозйомка;

— використання підслуховуючих пристроїв;

— захоплення та наведення електромагнітного випромінювання тощо.

2-а група – канали доступу до елементів системи та зміни структури її компонентів.

До другої групи відносяться:

— спостереження за інформацією з метою її запам’ятовування під час обробки;

— викрадення носіїв інформації;

— збір промислових відходів, що містять оброблену інформацію;

— навмисне читання даних з файлів інших користувачів;

— зчитування залишкової інформації, тобто даних, що залишилися на носії після виконання завдань;

— копіювання мультимедіа;

— умисне використання терміналів зареєстрованих користувачів для отримання доступу до інформації;

— видавати себе за зареєстрованого користувача, викрадаючи паролі та інші дані для обмеження доступу до цінної інформації;

— за допомогою т.зв. «прогалини» в доступі до інформації, тобто можливість обходу механізму обмеження доступу, яка виникає внаслідок недосконалості програмних компонентів усієї системи (операційних систем, систем управління базами даних тощо);

— відсутність ясності в мовах програмування, які використовуються в автоматизованих системах обробки даних.

До *3 групи* включається:

— незаконне підключення спеціального записуючого пристрою до системних пристроїв або ліній зв’язку (перехоплення модемного та факсимільного зв’язку);

— зловмисна модифікація програм таким чином, що ці програми разом з основними функціями обробки інформації також виконують несанкціонований збір та запис захищеної інформації;

— зловмисне відключення захисних механізмів.

Група 4 включає несанкціоноване отримання інформації шляхом підкупу або шантажу посадових осіб відповідних структурних підрозділів,

службовців, їхніх знайомих, службовців або родичів, які знають про вид діяльності.

Одна з проблем безпеки при витоку є *мережева інформація*. Сильною стороною сучасних мереж і причиною їх використання для максимального використання обчислювальних ресурсів є здатність швидко передавати інформацію. Мережева інформація, отримана з бази даних або надіслана електронною поштою, може легко вийти з-під контролю. Вона може бути зібрана із, здавалося б, нешкідливих фрагментів даних у важливу інформацію, яка розкриває виробничі плани, маркетингові стратегії чи бізнес-плани. [1].

У цьому випадку є три способи витоку інформації.

По-перше, інформація може залишатися незахищеною в різних місцях мережі, що дозволяє допитливим користувачам, хакерам або промисловим шпигунам збирати інформацію. Навіть з відносно низьким рівнем доступу користувачі можуть перевірити сотні місць у мережі, які містять інформацію.

По-друге, адреса призначення може містити помилку, в результаті чого інформація буде надіслана не тому учаснику. Списки розсилки ще більш небезпечні, оскільки фактичні одержувачі відносно невидимі. У багатьох випадках користувачі локальної мережі не впевнені, чи відповідають члени списку розсилки поточній ситуації; деякі члени можуть бути поза мережею або навіть поза організацією.

По-третє, слабке управління може дозволити невідомим особам використовувати мережу. Приклади включають так звані гостьові облікові записи, які використовуються для демонстрації чи інших цілей. Якщо цілі виправдовують використання локальної мережі третіми особами, у таких випадках організація повинна запровадити ефективну авторизацію та контроль ідентифікації.

Стосовно електронної комерції, *шахрайство* з оплатою, більш відоме як Payment Fraud – це спроба здійснити шахрайську або незаконну транзакцію. Поширені сценарії включають шахрайство з кредитними картками, помилкове

повернення та трикутне шахрайство (triangle scam). Трикутне шахрайство полягає в тому, що зловмисник відкриває інтернет-магазин із дуже низькими цінами, обманом змушує клієнтів надати свою платіжну інформацію, а потім використовує цю платіжну інформацію для покупки продуктів в інших магазинах.

Коли витік даних відбувається з ініціативи кіберзлочинців, це зазвичай є результатом тактики *соціальної інженерії*.

Соціальна інженерія – це використання психологічних маніпуляцій, щоб обманом змусити жертв надати конфіденційну інформацію. Фішинг є найпоширенішим типом атак соціальної інженерії. Традиційно фішинг має форму повідомлення з проханням до користувача надати конфіденційну інформацію або виконати дію, вигідну для зловмисника. Все частіше фішинг здійснюється по телефону.

Дуже часто зловмисники шукають дані, які самі по собі не є конфіденційними, але можуть розширити список потенційних жертв. Це створює серйозну загрозу безпеці даних, оскільки зловмисники можуть легко обдурити нічого непідозрюючих співробітників, запитуючи на перший погляд нешкідливу інформацію, таку як номери телефонів і номери соціального страхування.

Хоча спам і фішингові атаки не обов'язково є складними з технологічної точки зору, вони покладаються на складну тактику соціальної інженерії, що робить їх дуже небезпечними для тих, хто про них не знає. Шахраї вміють створювати фішингові веб-сторінки, ідентичні оригінальним веб-сайтам, які збирають особисті дані користувачів або заохочують переказ грошей шахраям, націленим як на окремих осіб, так і на організації. Експерти Kaspersky виявили, що протягом 2022 року кіберзлочинці все частіше зверталися до фішингу. Антифішингова система компанії успішно заблокувала 507 851 735 спроб отримати доступ до шахрайського контенту в 2022 році, що вдвічі перевищує кількість атак, зірваних у 2021 році.

Найчастіше жертвами фішингових атак стали користувачі служб доставки, на них припало 27,38% усіх заблокованих спроб. Шахраї надсилають фальшиві електронні листи, нібито від відомих кур'єрських компаній, і стверджують, що з доставкою виникли проблеми. Електронний лист містить посилання на фальшивий веб-сайт, який запитує особисту інформацію або фінансові деталі. Якщо жертва попадеться на шахрайство, вона може втратити свою особу та банківську інформацію, яка може бути продана веб-сайтам у темній мережі. Серед інших популярних об'єктів фішингових атак – інтернет-магазини (15,56%), платіжні системи (10,39%) і банки (10,39%).

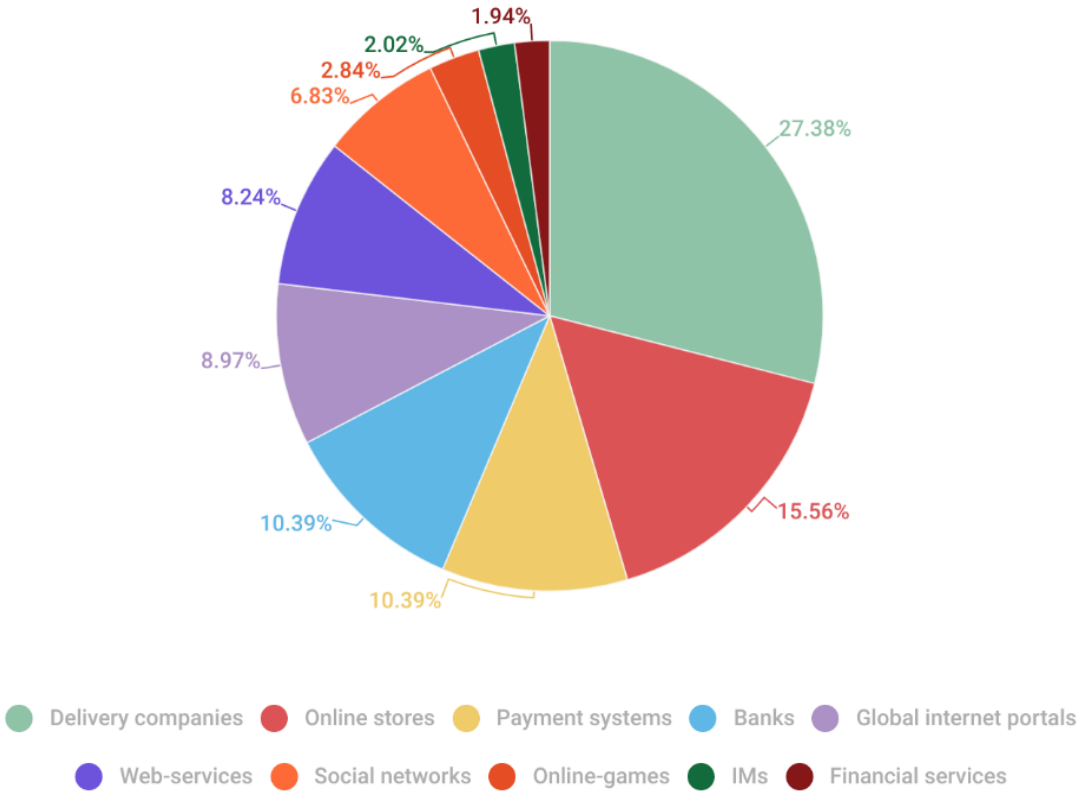

Рисунок 1.1 - Розподіл організацій, на яких націлений фішинг, за категоріями, 2022 рік [2]

Багато витоків інформації спричинені не атаками, а скоріше ненавмисним розкриттям конфіденційної інформації. Зазвичай пристрої організації містять конфіденційну інформацію, і неправильне використання

цих пристроїв може призвести до порушення безпеки та викрадення інформації компанії. Наприклад, кіберзлочинець може використати викрадений пристрій, щоб зв’язатися з IT-адміністратором і заявити, що він забув свої дані для входу. За допомогою переконливої стратегії зловмисники можуть зламати пристрій і отримати доступ до корпоративної мережі. Або, співробітники можуть переглядати конфіденційні дані та зберігати їх у незахищеному місці, або IT-спеціалісти можуть помилково надати конфіденційний внутрішній сервер або хмарну систему.

Але ще одна проблема - *внутрішні загрози*, що включають незадоволених співробітників, колишніх співробітників, які мають доступ до конфіденційних систем, або ділових партнерів. Їхніми мотивами може бути економічна вигода, крадіжка цінної інформації або бажання помститися. Інсайдери можуть викрасти конфіденційну інформацію організації з метою фінансової чи особистої вигоди.

Численні організації надають співробітникам такі привілеї, як доступ до Інтернету, електронна пошта та обмін миттєвими повідомленнями. Однак занепокоєння виникає через те, що всі ці канали зв'язку мають можливість передавати файли або підключатися до зовнішніх джерел через публічні мережі. Зловмисники часто націлюються на ці канали зв’язку та досягають високого рівня успіху. Наприклад, кіберзлочинець може підробити стандартну електронну пошту та просто попросити співробітника надіслати йому конфіденційну інформацію. Якщо повідомлення вводить в оману користувача, він може прикріпити запитувані файли до електронного листа та надіслати їх зловмиснику.

1.2 Загальні заходи по забезпеченню безпеки

Для запобігання витоку даних, першим кроком є визначення того, якими даними працівники можуть вільно ділитися. Потім повинні вирішити, хто

повинен мати дозвіл на доступ до цих даних. Використовуючи ідентифікацію та класифікацію даних, можливо організувати дані за категоріями, захищаючи конфіденційні дані за потреби. [3].

Щоб запобігти витоку даних і підвищити загальну безпеку, організації повинні розглянути можливість впровадження таких загальних заходів безпеки:

1. *Безпека мережі.* Використовувати брандмауери та системи виявлення/попередження вторгнень (IDS/IPS) для моніторингу та контролю мережевого трафіку. Використовуйте безпечні мережеві конфігурації та сегментацію, щоб звести до мінімуму неавторизований доступ. Застосувати надійні протоколи автентифікації мережі, наприклад WPA2 або WPA3 для мереж WiFi.

2. *Автентифікація користувача та контроль доступу.* Застосувати політику надійних паролів, включаючи вимоги щодо складності та регулярних змін паролів. Активувати багатофакторну автентифікацію (MFA), щоб додати додатковий рівень безпеки для входу користувачів. Діяти згідно до принципу найменших привілеїв, надаючи користувачам лише необхідні права доступу для їхніх ролей.

3. *Навчання та обізнаність співробітників.* Провести для співробітників всебічне навчання з питань безпеки, навчіть їх щодо захисту даних, фішингових атак і соціальної інженерії. Навчити співробітників безпечно поводитися з конфіденційною інформацією та повідомляти про підозрілу діяльність.

4. *Шифрування даних*. Шифрувати конфіденційні дані під час передачі та передачі за допомогою надійних алгоритмів і протоколів шифрування. Застосувати шифрування для даних, що зберігаються на портативних пристроях, таких як ноутбуки, смартфони або USB-накопичувачі.

5. *Безпека кінцевої точки.* Розгорнути та регулярно оновлювати антишкідливе програмне забезпечення/антивірусне програмне забезпечення

на всіх кінцевих точках. Запровадити шифрування пристрою та застосувати політики для безпечного керування пристроєм. Увімкнути дистанційне відстеження та можливості видалення даних для втрачених або викрадених пристроїв.

6. *Фізична безпека.* Безпечний фізичний доступ до серверних кімнат, центрів обробки даних та іншої критичної інфраструктури. Впровадити відеоспостереження, системи контролю доступу та протоколи керування відвідувачами.

7. *Реагування на інциденти та моніторинг.* Створити план реагування на інциденти, щоб швидко й ефективно впоратися з інцидентами безпеки. Впровадити системи моніторингу в реальному часі, щоб виявляти підозрілі дії або спроби несанкціонованого доступу та реагувати на них. Регулярно переглядати та аналізувати журнали та події безпеки на наявність потенційних загроз або ознак компрометації.

8. *Безпечна розробка програмного забезпечення.* Дотримуватись правил безпечного кодування та регулярно перевіряйте код безпеки та оцінюйте вразливості. Підтримувати програмне забезпечення та програми в актуальному стані за допомогою останніх виправлень безпеки та оновлень. Провести ретельне тестування безпеки, включаючи тестування на проникнення та сканування вразливостей.

9. *Резервне копіювання та відновлення даних.* Регулярно створювати резервні копії критично важливих даних і тестувати процес відновлення, щоб переконатися, що дані можна відновити у разі їх втрати або зламу. Надійно зберігати резервні копії та відокремлюйте їх від робочого середовища.

10. *Відповідність і правила.* Бути в курсі відповідних норм захисту даних і галузевих стандартів. Впровадити необхідні засоби контролю та процеси для дотримання чинних законів, таких як GDPR, CCPA або HIPAA. Пам’ятати, що заходи безпеки слід впроваджувати на основі багаторівневого підходу, поєднуючи технічний контроль, політики та обізнаність

співробітників, щоб ефективно запобігти витоку даних і захистити конфіденційну інформацію. Регулярні оцінки безпеки, аудити та безперервний моніторинг є важливими для підтримки надійної безпеки.

1.3 Постановка завдання

Метою роботи є аналіз витоків даних в популярних компаніях, а саме знаходження основних факторів і каналів витоку інформації, розгляд загальних заходів по забезпеченню безпеки та методи запобігання витоку даних.

Об'єктом роботи є реалізація запитів до пошукових систем, що знаходить злиті акаунтів на основі домену організації.

Предмет роботи: зламані аккаунти та супутня до них інформація.

Для досягнення поставленої мети необхідно вирішити наступні *завдання*:

– Аналіз витоку даних та методів запобігання витоку даних організації.

– Огляд доменів популярних компаній.

– Аналіз та виявлення злитих акаунтів, які належать цьому домену.

– На основі проведеного аналізу створити скріпт, який реалізує запити для пошуку злитих акаунтів на домені організації.

2. МЕТОДИ ЗАПОБІГАННЯ ВИТОКУ ДАНИХ

2.1 Витікаючий веб-трафік

Вихідний веб-трафік стосується даних, що передаються з пристрою або мережі користувача на віддалені сервери або пункти призначення в Інтернеті за допомогою різних протоколів, таких як HTTP, FTP, P2P тощо. Вихідний веб-трафік, включно з цими протоколами, може становити загрозу безпеці та витоку даних, якщо його не відстежувати чи контролювати належним чином. Організації часто впроваджують заходи для керування вихідним веб-трафіком, щоб захистити конфіденційну інформацію та застосувати політику безпеки. Серед поширених методів:

1. Правила брандмауера: брандмауери можна налаштувати для моніторингу та контролю вихідного веб-трафіку на основі попередньо визначених правил. Ці правила можуть обмежувати доступ до певних портів, протоколів або місць призначення, щоб запобігти неавторизованому або небажаному трафіку.

2. Проксі-сервери: проксі-сервери діють як посередники між клієнтами та веб-серверами. Їх можна налаштувати для перевірки та фільтрації вихідного веб-трафіку, дозволяючи організаціям застосовувати політики безпеки, обмежувати доступ до певних веб-сайтів або протоколів і реєструвати дії користувачів.

3. Системи виявлення/запобігання вторгненням (IDS/IPS): системи IDS/IPS відстежують мережевий трафік і можуть виявляти та запобігати потенційно зловмисному або неавторизованому вихідному веб-трафіку. Вони можуть ідентифікувати та блокувати підозрілі дії, такі як викрадання даних або зв’язок із відомими шкідливими серверами.

4. Системи запобігання втраті даних (DLP): системи DLP можуть аналізувати вихідний веб-трафік на наявність конфіденційної інформації,

наприклад конфіденційних документів або особистої інформації (PII). Вони можуть застосувати політику для запобігання передачі конфіденційних даних або застосувати заходи шифрування для їх захисту.

5. Фільтрування вмісту. Системи фільтрування вмісту можна використовувати для блокування або обмеження доступу до певних веб-сайтів, категорій веб-сайтів (наприклад, соціальні мережі, азартні ігри) або типів вмісту. Це допомагає організаціям підтримувати продуктивність, зменшувати ризики безпеки та застосовувати прийнятні політики використання.

6. Шифрування: під час передачі конфіденційних даних через такі протоколи, як HTTP або FTP, використання механізмів шифрування, таких як HTTPS або FTPS, додає додатковий рівень безпеки. Шифрування забезпечує безпечну передачу даних і захист від перехоплення або несанкціонованого доступу.

Організаціям важливо застосовувати комбінацію цих методів для ефективного керування та захисту вихідного веб-трафіку, захисту конфіденційних даних, пом’якшення ризиків і забезпечення відповідності політикам і нормам безпеки. [4].

2.1.1 HTTP (протокол передачі гіпертексту)

HTTP — це протокол, який використовується для передачі веб-сторінок, зображень, файлів та інших ресурсів через Інтернет. [5]. Це основа передачі даних у Всесвітній павутині. HTTP працює через порт 80 для незашифрованого трафіку та порт 443 для зашифрованого трафіку за допомогою HTTPS (HTTP Secure).

Коли використовується протокол HTTP (Hypertext Transfer Protocol) для передачі даних між клієнтом (наприклад, веб-браузером) та сервером, веб-трафік може витікати і стати доступним незаконним особам. Витік веб-трафіку

при використанні HTTP може мати серйозні наслідки, оскільки цей протокол передає дані у незашифрованому вигляді. Ось деякі аспекти, пов'язані з витоком веб-трафіку при використанні протоколу HTTP:

1. Незашифрована передача даних: HTTP передає дані у відкритому текстовому форматі, що означає, що інформація, яку ви передаєте через веб-сайти, включаючи логіни, паролі, особисті дані та іншу конфіденційну інформацію, може бути перехоплена і прочитана третіми особами.

2. Можливість встановлення перехопленого з'єднання: зловмисники можуть використовувати техніки, такі як атака "Man-in-the-Middle" (чоловік посередині), для перехоплення веб-трафіку між клієнтом і сервером. Це дозволяє зловмисникам переглядати та модифікувати передані дані.

3. Небезпека перехоплення сесій: у випадку витоку веб-трафіку, включаючи кукі (cookies), які містять інформацію про сесію користувача, зловмисники можуть отримати доступ до облікових записів користувачів і використовувати їх для несанкціонованого доступу до різних сервісів.

4. Небезпека шпигунства і перехоплення даних: зловмисники можуть перехоплювати веб-трафік для збору конфіденційних даних, таких як банківські реквізити, особисті дані або комерційна інформація. Ця інформація може бути використана для шпигунства, шахрайства, вимагання викупу або інших злочинних цілей.

Однак, є кілька методів, які можна використовувати для попередження витоку веб-трафіку при використанні протоколу HTTP:

1. Використання HTTPS: HTTPS (Hypertext Transfer Protocol Secure) є захищеним варіантом протоколу HTTP, де дані передаються у зашифрованому вигляді за допомогою SSL або TLS протоколу. Використання HTTPS дозволяє захистити передачу конфіденційних даних, таких як логіни та паролі, від перехоплення.

2. Використання шифрування на рівні даних: для додаткового захисту конфіденційних даних можна використовувати шифрування на рівні

даних. Це означає, що дані шифруються перед їх передачею і розшифровуються лише на стороні отримувача.

3. Використання захищених кукі: якщо необхідно використовувати кукі для зберігання ідентифікаційних даних або стану сесії, рекомендується використовувати захищені кукі, які передаються лише через зашифроване з'єднання HTTPS і мають встановлені відповідні атрибути безпеки.

4. Використання мережевих заходів безпеки: для попередження витоку веб-трафіку можна використовувати різні мережеві заходи безпеки, такі як брандмауери, виявлення та запобігання вторгненням (IDS/IPS), веб-фільтри та системи захисту від DDoS-атак. Ці заходи можуть допомогти виявити та блокувати небезпечний веб-трафік.

5. Освіта та свідомість користувачів: важливо навчати користувачів про основні принципи безпеки в Інтернеті, зокрема про ризики витоку веб-трафіку при використанні протоколу HTTP. [6]. Користувачам слід наголошувати на важливості використання безпечних з'єднань, таких як HTTPS, при взаємодії з веб-сайтами, особливо при введенні конфіденційної інформації.

6. Аудит безпеки: проведення регулярного аудиту безпеки веб-сайту та його інфраструктури може допомогти виявити потенційні уразливості, які можуть призвести до витоку веб-трафіку. Це дозволить прийняти відповідні заходи з попередження витоку даних.

7. Моніторинг трафіку та виявлення загроз: застосування систем моніторингу трафіку та виявлення загроз може допомогти виявити підозрілий або аномальний веб-трафік, що може свідчити про спроби витоку даних. Це дозволяє швидко реагувати на потенційні загрози та запобігати витоку даних.

8. Регулярні оновлення та патчі: важливо підтримувати всі програмні компоненти, використовувані на веб-сайті, у актуальному стані, встановлюючи оновлення та патчі безпеки. [7]. Це допоможе усунути відомі уразливості, які можуть бути використані для витоку даних.

Загалом, поєднання технічних заходів безпеки, використання шифрування та свідомість користувачів щодо безпеки в Інтернеті є важливими для попередження витоку веб-трафіку при використанні протоколу HTTP.

2.1.2 FTP (протокол передачі файлів)

FTP — це стандартний мережевий протокол, який використовується для передачі файлів між клієнтом і сервером. Він забезпечує простий спосіб завантаження, завантаження та керування файлами на віддалених серверах. FTP зазвичай працює на порту 21 для керування та використання додаткових портів для передачі даних. [8].

Коли використовується протокол FTP (File Transfer Protocol) для передачі файлів між клієнтом і сервером, веб-трафік також може витікати і стати доступним незаконним особам. Протокол FTP передає дані у незашифрованому вигляді, що робить його вразливим до перехоплення та несанкціонованого доступу. Ось деякі аспекти, пов'язані з витоком веб-трафіку при використанні протоколу FTP:

1. Незахищена передача даних: протокол FTP передає дані у відкритому текстовому форматі, включаючи логіни, паролі та іншу конфіденційну інформацію. Це означає, що дані можуть бути перехоплені зловмисниками, які мають доступ до мережі, через яку проходить з'єднання.
2. Витік логін-даних: коли клієнт встановлює з'єднання з FTP-сервером, логін-дані, такі як ім'я користувача та пароль, передаються у відкритому вигляді. Це означає, що зловмисники можуть перехопити ці дані і використовувати їх для несанкціонованого доступу до системи.
3. Відсутність шифрування: протокол FTP не має вбудованої підтримки шифрування для захисту передачі даних. Це робить його вразливим до прослуховування трафіку та перехоплення даних зловмисниками.

4. Ризик перехоплення файлів: крім логін-даних, самі файли, які передаються через протокол FTP, можуть бути перехоплені зловмисниками. Це може стати проблемою, якщо файли містять конфіденційну або приватну інформацію.

5. Небезпека використання активного режиму: Протокол FTP має два режими передачі - активний і пасивний. Активний режим в протоколу FTP вимагає встановлення додаткових з'єднань між клієнтом і сервером для передачі даних. Це може створювати додаткові точки вразливості, оскільки зловмисники можуть використовувати ці з'єднання для перехоплення трафіку або атаки на систему.

Щоб попередити витік веб-трафіку при використанні протоколу FTP і забезпечити більшу безпеку, можна застосовувати такі методи:

1. Використання захищених варіантів FTP: нативний протокол FTP не є безпечним. Однак, існують розширення та реалізації протоколу, такі як FTPS (FTP over SSL/TLS) і SFTP (SSH File Transfer Protocol), які забезпечують шифрування трафіку за допомогою SSL/TLS або SSH. Використання FTPS або SFTP забезпечує захищену передачу даних через FTP.

2. Використання VPN: використання віртуальної приватної мережі (VPN) може додатково захистити передачу даних через FTP. VPN шифрує весь трафік між клієнтом і сервером, включаючи FTP-з'єднання, тим самим забезпечуючи конфіденційність і захист даних.

3. Використання обмежень доступу і аутентифікації: для запобігання несанкціонованому доступу до FTP-сервера важливо встановити міцні паролі, використовувати методи аутентифікації з використанням шифрування, імплементувати механізми блокування після некоректних спроб аутентифікації та обмеження доступу до файлів на основі рівнів авторизації.

4. Моніторинг трафіку і виявлення загроз: регулярний моніторинг FTP-трафіку та використання систем виявлення загроз можуть допомогти виявити незвичайну або підозрілу активність на FTP-сервері, яка може

свідчити про можливий витік даних або несанкціонований доступ. Такі системи можуть сповіщати про підозрілі дії або спроби несанкціонованого доступу, що дозволяє прийняти вчасні заходи для запобігання витоку даних.

5. Застосування обмежень на рівні мережі: використання брандмауерів, правил файрвола та інших мережевих засобів безпеки дозволяє контролювати доступ до FTP-сервера. Обмеження можуть бути встановлені на основі IP-адрес, [9], портів, протоколів або інших параметрів, що дозволяють обмежити доступ до FTP-сервера тільки для авторизованих користувачів або з визначеними довіреними діапазонами IP-адрес.

6. Регулярні оновлення та патчі: підтримка оновленої версії FTP-сервера і використання останніх патчів і виправлень допомагають усунути відомі уразливості та захистити систему від атак і витоку даних.

7. Свідомість користувачів: важливо навчати користувачів про безпеку використання FTP, зокрема про ризики витоку даних та заходи безпеки, такі як використання захищених варіантів протоколу FTP, міцні паролі та обмеження доступу.

Загалом, витік веб-трафіку при використанні протоколу FTP може бути проблемою з точки зору безпеки. Важливо застосовувати вищезазначені методи та рекомендації для забезпечення захищеної передачі даних та попередження витоку веб-трафіку.

2.1.3 P2P (Peer-to-Peer)

P2P — це децентралізована мережева архітектура, де учасники (однорангові вузли) можуть безпосередньо обмінюватися файлами та ресурсами один з одним, не покладаючись на центральний сервер. Протоколи P2P, такі як BitTorrent, полегшують розповсюдження та обмін файлами в одноранговій мережі.

При використанні протоколу P2P (Peer-to-Peer) веб-трафік може витікати через різні механізми. Протокол P2P передбачає безпосередню комунікацію між вузлами мережі, що може створювати певні ризики з точки зору безпеки. Ось кілька аспектів, пов'язаних з витоком веб-трафіку при використанні протоколу P2P:

1. Незахищені з'єднання: багато P2P-програм та протоколів, таких як BitTorrent, використовують незахищені з'єднання, що означає, що дані передаються у відкритому вигляді. Це може дозволити зловмисникам перехоплювати та читати передані дані.

2. Публічні IP-адреси: більшість P2P-протоколів вимагають використання публічних IP-адрес, що може робити вашу систему більш видимою в Інтернеті. Це може зробити вас більш вразливими до зловмисників і злочинних елементів, які можуть спробувати використати цю видимість для атак або витоку даних.

3. Витік конфіденційної інформації: використання P2P-протоколів, особливо для обміну файлами, може призвести до витоку конфіденційної інформації. Якщо файли, які ви обмінюєте, містять особисті дані, комерційну інформацію або іншу конфіденційну інформацію, вони можуть бути доступні для незаконних осіб, які беруть участь у P2P-мережі.

4. Ризик шкідливого програмного забезпечення: оскільки протокол P2P дозволяє безпосередню комунікацію між вузлами мережі, існує ризик зараження шкідливим програмним забезпеченням. Зловмисники можуть використовувати P2P-мережу для поширення шкідливих файлів або впровадження вразливостей через підроблені файли. Якщо користувач неправильно обмінюється файлами через P2P-мережу, це може призвести до витоку даних або інфікування своєї системи шкідливим програмним забезпеченням.

Заходи для попередження витоку веб-трафіку при використанні протоколу P2P включають:

1. Використання надійного та актуалізованого програмного забезпечення: використовуйте довірчі програми P2P, які регулярно оновлюються та мають добру репутацію. Переконайтеся, що встановлене антивірусне програмне забезпечення оновлене і активне на вашій системі.

2. Контроль вмісту, який ви обмінюєте: будьте уважні щодо файлів, які ви обмінюєте через P2P-мережу. Уникайте сумнівних або неперевірених джерел. Перед завантаженням або відкриттям файлу перевірте його на наявність шкідливого програмного забезпечення за допомогою антивірусного сканера.

3. Керування налаштуваннями приватності: багато програм P2P мають налаштування приватності та безпеки. Використовуйте ці налаштування для обмеження доступу до вашої системи або вибірного обміну файлами лише з надійними користувачами.

4. Використання VPN: використання віртуальної приватної мережі (VPN) може забезпечити шифрування вашого з'єднання та приховати вашу IP-адресу. Це допоможе підвищити безпеку та конфіденційність під час використання P2P-протоколу.

5. Моніторинг активності мережі: слід регулярно моніторити активність вашої мережі, включаючи P2P-протоколи, за допомогою спеціалізованих інструментів або мережевих моніторів. Це дозволяє виявити незвичайну або підозрілу активність, яка може вказувати на витік даних або несанкціонований обмін.

6. Захист мережі за допомогою брандмауерів і IDS/IPS: використання брандмауерів (файрволів) та систем виявлення/запобігання вторгнення (IDS/IPS) може допомогти контролювати трафік P2P, блокувати небажаних користувачів або небезпечні підключення, а також спостерігати за підозрілими діями.

7. Криптографічне шифрування: при використанні P2P-протоколів розгляньте можливість шифрування передачі даних. Використання

криптографічних методів шифрування може забезпечити конфіденційність та цілісність передачі даних, запобігаючи несанкціонованому доступу і витоку інформації.

8. Контроль доступу і автентифікація: встановлення строгого контролю доступу до вашої P2P-мережі шляхом використання автентифікації і авторизації допоможе уникнути несанкціонованого доступу та витоку даних. Використовуйте надійні паролі, обмежуйте доступ лише для авторизованих користувачів і регулярно оновлюйте ідентифікаційні дані.

9. Оновлення та патчі: підтримка оновленої версії P2P-програмного забезпечення та вчасне встановлення патчів і оновлень допоможе усунути відомі уразливості і зменшити ризик витоку веб-трафіку при використанні протоколу P2P:

10. Освіта та свідоме користування: важливо бути освіченим щодо ризиків, пов'язаних з використанням P2P-протоколів, і свідомо підходити до обміну файлами та використання мережі. Навчіться розпізнавати потенційно шкідливі файли та ризикові ситуації, і бережіться сумнівних джерел або небезпечних дій.

11. Резервне копіювання даних: забезпечте регулярне резервне копіювання ваших даних. Якщо станеться витік або втрата даних через P2P-мережу, ви зможете відновити їх з резервних копій.

12. Моніторинг і аналіз мережі: використання мережевих інструментів для моніторингу та аналізу P2P-трафіку може допомогти виявити небажану або підозрілу активність, а також вчасно реагувати на можливі проблеми з безпекою.

13. Створення політик безпеки: розробіть і виконуйте політики безпеки для використання P2P-мережі. Ці політики можуть включати обмеження на використання певних протоколів, контроль доступу, регулярну оцінку ризиків і навчання користувачів.

14. Співпраця з постачальниками послуг: якщо ви використовуєте P2P-програми або протоколи в організаційному контексті, співпрацюйте з постачальниками послуг або мережевими адміністраторами для впровадження заходів безпеки, контролю трафіку та моніторингу активності.

Загальною стратегією для попередження витоку веб-трафіку при використанні протоколу P2P є забезпечення комплексного підходу до безпеки. Це включає поєднання технічних заходів, які включають в себе захист мережі, шифрування даних і контроль доступу, а також освіту користувачів і свідоме використання P2P-мережі.

Важливо розуміти, що безпека використання протоколу P2P є взаємодійним завданням між користувачами і постачальниками послуг. Користувачі повинні дотримуватися найкращих практик безпеки, таких як перевірка файлів перед завантаженням, встановлення актуального антивірусного програмного забезпечення і обережне обмінюватися даними. Постачальники послуг повинні надати засоби для контролю та моніторингу трафіку, реалізувати політики безпеки і забезпечувати оновлення програмного забезпечення та захисних механізмів.

Загалом, зрозуміння потенційних ризиків і прийняття відповідних заходів безпеки можуть допомогти уникнути витоку веб-трафіку при використанні протоколу P2P.

2.2 Вихідна електронна пошта, внутрішня електронна пошта

Вхідна електронна пошта – це повідомлення, отримані особою чи організацією від зовнішніх відправників через протокол електронної пошти. З іншого боку, внутрішня електронна пошта стосується повідомлень, якими обмінюються особи в одній організації. Ось деяка інформація про керування вхідною та внутрішньою електронною поштою:

1. Фільтрування електронної пошти: впровадження систем фільтрації

електронної пошти, наприклад фільтрів спаму, може допомогти блокувати небажані та потенційно шкідливі електронні листи. Ці фільтри використовують різні методи, зокрема чорні списки, білі списки, аналіз вмісту та алгоритми машинного навчання, щоб ідентифікувати та сортувати вхідні електронні листи на основі їх легітимності та потенційних ризиків.

2. Антивірусне сканування та сканування від зловмисного програмного забезпечення. Сканування вхідних вкладень електронної пошти та вбудованих посилань на наявність вірусів, зловмисного програмного забезпечення та іншого шкідливого вмісту має вирішальне значення. Розгортання антивірусного програмного забезпечення та програмного забезпечення для захисту від шкідливих програм допомагає виявляти та блокувати будь-які загрози до того, як вони можуть завдати шкоди системі чи мережі одержувача.

3. Автентифікація електронної пошти. Застосування протоколів автентифікації електронної пошти, таких як Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) і Domain-based Message Authentication, Reporting, and Conformance (DMARC), може допомогти перевірити автентичність і цілісність вхідних електронних листів. Ці протоколи гарантують легітимність відправника та запобігають спуфінгу електронної пошти та фішинговим атакам.

4. Обізнаність і навчання користувачів: необхідно ознайомити користувачів із найкращими методами безпеки електронної пошти. Програми навчання можуть навчити користувачів виявляти та уникати підозрілих електронних листів, спроб фішингу та методів соціальної інженерії. Слід заохочувати користувачів бути обережними, відкриваючи вкладення електронної пошти, натискаючи посилання або надсилаючи конфіденційну інформацію електронною поштою.

5. Шифрування: запровадження протоколів шифрування електронної пошти, таких як Transport Layer Security (TLS) або Pretty Good Privacy (PGP), додає додатковий рівень безпеки до вхідних і внутрішніх електронних листів.

Шифрування гарантує, що вміст електронних листів захищено від несанкціонованого доступу або перехоплення під час передачі.

6. Архівування та зберігання електронної пошти: організації часто мають юридичні вимоги та вимоги дотримання нормативних вимог щодо зберігання електронних листів протягом певного періоду. Впровадження рішень для архівування електронної пошти допомагає зберігати та керувати вхідними та внутрішніми електронними листами в безпечний спосіб із можливістю пошуку, забезпечуючи відповідність і полегшуючи пошук у разі потреби.

7. Політика використання електронної пошти: встановлення чіткої політики використання електронної пошти може допомогти керувати тим, як обробляються вхідні та внутрішні електронні листи в організації. У цих політиках можна окреслити вказівки щодо прийнятного використання, вмісту електронної пошти, обробки вкладених файлів і належного поводження з конфіденційною інформацією.

8. Моніторинг електронної пошти та реагування на інциденти: впровадження систем моніторингу електронної пошти дозволяє організаціям виявляти потенційні інциденти безпеки або порушення політики та реагувати на них. Відстеження трафіку електронної пошти може допомогти виявити незвичайні закономірності, виявити спроби несанкціонованого доступу та вжити оперативних заходів для зменшення ризиків.

Впроваджуючи ці заходи, організації можуть ефективно керувати вхідною та внутрішньою електронною поштою, захищати від загроз і забезпечувати конфіденційність, цілісність і доступність електронної пошти.

2.3 Системи миттєвого обміну повідомленнями

Миттєвий обмін повідомленнями надає можливість надсилати текстові повідомлення, як правило, короткі у швидкій послідовності, між колегами по

бізнесу та особистими друзями. Це дозволяє вести розмову в реальному часі без використання телефону. Крім того, миттєві повідомлення надають індикатор, який показує, чи перебуває інша особа в мережі та чи доступна для спілкування.

Обмін миттєвими повідомленнями — це програма з підтримкою електронної пошти двома способами:

— Індикатор присутності в папці "Вхідні". Коли ви переглядаєте список нових електронних листів у своїй папці "Вхідні", ваша служба обміну миттєвими повідомленнями може вказати, чи перебувають відправники останніх електронних листів у мережі в цей конкретний час. Якщо так, ви можете розпочати сеанс обміну миттєвими повідомленнями, щоб поставити конкретне додаткове запитання щодо електронного листа, який ви щойно отримали.

— Індикатор присутності в повідомленні електронної пошти. Коли ви відкриваєте повідомлення електронної пошти від колеги, індикатор присутності може бути вбудований у повідомлення, який показує статус доступності особи в певний час. Одержувач може натиснути індикатор присутності, щоб автоматично розпочати сеанс миттєвих повідомлень із початковим відправником.

Системи обміну миттєвими повідомленнями широко використовуються для спілкування в реальному часі та співпраці в організаціях. Ось деякі методи щодо керування системами обміну миттєвими повідомленнями:

1. Автентифікація та контроль доступу: запровадьте механізми автентифікації користувачів, щоб забезпечити доступ до системи обміну миттєвими повідомленнями лише авторизованим особам. Обліковими записами користувачів слід належним чином керувати за допомогою надійних паролів і періодичного оновлення паролів.

2. Шифрування: увімкніть наскрізне шифрування в системі обміну миттєвими повідомленнями, щоб захистити конфіденційність розмов.

Шифрування гарантує, що повідомлення доступні лише призначеним одержувачам і недоступні для неавторизованих сторін.

3. Політика та навчання користувачів: встановіть чітку політику щодо використання систем обміну миттєвими повідомленнями та донесіть її до користувачів. Навчіть співробітників найкращим практикам безпечного обміну повідомленнями, зокрема уникайте обміну конфіденційною інформацією та обережно натискайте підозрілі посилання чи завантажуйте вкладення.

4. Зберігання та архівування даних: визначте політику збереження даних вашої організації для розмов миттєвих повідомлень. Деякі галузі мають нормативні вимоги щодо зберігання журналів чату протягом певного періоду. Застосуйте механізми архівування для зберігання та отримання історії чату, коли це необхідно.

5. Керування мобільними пристроями (MDM): якщо співробітники використовують програми обміну миттєвими повідомленнями на своїх мобільних пристроях, подумайте про впровадження рішень MDM для забезпечення дотримання політик безпеки, керування встановленням програм і віддаленого видалення даних із втрачених або викрадених пристроїв.

2.4 Мережевий та локальний друк

Інфраструктура друку в організації може становити загрозу безпеці. Ось деякі міркування щодо керування мережевим і локальним друком:

1. Захищений друк: реалізуйте рішення для безпечного друку, наприклад автентифікацію користувача на принтері, щоб запобігти несанкціонованому доступу до друкованих документів. Це гарантує, що конфіденційна інформація не потрапить у чужі руки.

2. Контроль доступу до принтерів: контролюйте фізичний доступ до принтерів, розміщуючи їх у безпечних місцях і обмежуючи доступ лише

авторизованому персоналу. Регулярно переглядайте та оновлюйте права доступу до принтерів.

3. Моніторинг завдань друку: запровадьте системи моніторингу завдань друку, щоб відстежувати та перевіряти діяльність друку. Це допомагає виявити будь-який підозрілий або неавторизований друк і дає змогу організаціям вжити відповідних заходів.

4. Шифрування даних. Якщо конфіденційна інформація надсилається на принтери через мережу, увімкніть протоколи шифрування, щоб захистити конфіденційність даних, що передаються.

5. Оновлення мікропрограми та безпеки принтера: регулярно оновлюйте мікропрограму та програмне забезпечення принтера, щоб усунути будь-які вразливості безпеки. Будьте в курсі оновлень системи безпеки та негайно застосовуйте їх.

6. Безпечна утилізація: запровадьте процедури безпечної утилізації друкованих документів. Подрібнення або безпечна утилізація конфіденційних документів запобігає несанкціонованому доступу до викинутих матеріалів.

7. Політика використання принтера та навчання: установіть політику щодо використання принтера, включаючи вказівки щодо друку конфіденційної інформації, обробки роздруківок і належного використання спільних принтерів. Розкажіть співробітникам про цю політику та навчіть їх методам безпечного друку.

Впроваджуючи ці заходи, організації можуть покращити безпеку систем обміну миттєвими повідомленнями, мережевого друку та локальної інфраструктури друку, зменшуючи ризики, пов’язані з витоком даних і несанкціонованим доступом.

2.5 Контроль доступу до пристроїв та портів введення-виведення

Контроль доступу до пристроїв і портів введення/виведення має

вирішальне значення для забезпечення безпеки комп’ютерних систем і захисту конфіденційних даних. Доступ до портів і пристроїв вводу/виводу означає можливість взаємодії з портами вводу/виводу (I/O) і пристроями комп’ютерної системи. Ці порти та пристрої полегшують зв’язок із зовнішніми пристроями, такими як пристрої USB, послідовні порти, мережеві інтерфейси та інші периферійні пристрої. Керування доступом до цих портів і пристроїв є важливим для безпеки та контролю потоку даних.

Ось деякі зауваження щодо керування доступом до портів і пристроїв вводу/виводу:

1. Політики контролю доступу: визначте політики контролю доступу, які визначають, хто має дозвіл на доступ і використання певних портів і пристроїв. Ці політики можуть базуватися на ролях користувачів, посадових функціях або конкретних вимогах безпеки. Регулярно переглядайте та за потреби оновлюйте ці політики.

2. Автентифікація користувача: запровадьте механізми автентифікації користувачів, такі як надійні паролі, двофакторну автентифікацію (2FA) або біометричну автентифікацію, щоб гарантувати, що лише авторизовані особи можуть отримати доступ і використовувати порти та пристрої.

3. Білий список портів і пристроїв: схвалені порти та пристрої, які дозволено використовувати в системі, складають білий список. Цей підхід обмежує доступ лише авторизованим і надійним пристроям, зменшуючи ризик підключення неавторизованих або шкідливих пристроїв.

4. Чорний список портів і пристроїв: ведіть чорний список портів і пристроїв, які заборонено використовувати в системі. Це може включати порти чи пристрої, які становлять загрозу безпеці або не схвалені для використання в організації.

5. Контроль доступу на основі ролей (RBAC): запровадьте RBAC для призначення дозволів і прав доступу до певних портів і пристроїв на основі ролей або обов’язків користувачів. Це гарантує, що люди мають доступ лише

до портів і пристроїв, необхідних для виконання їхніх робочих функцій.

6. Моніторинг і журналювання: запровадьте механізми моніторингу та журналювання для відстеження дій портів і пристроїв. Це дає змогу виявляти будь-які спроби несанкціонованого доступу, підозрілі дії або витоки даних, пов’язані з портами та пристроями.

7. Регулярні оновлення та виправлення: оновлюйте мікропрограми, драйвери та операційні системи портів і пристроїв за допомогою останніх виправлень безпеки. Це допомагає усунути відомі вразливості та зменшити ризик використання.

8. Фізична безпека: захистить фізичний доступ до портів і пристроїв, захистивши фізичне середовище. Застосуйте такі заходи, як замкнені шафи, зони обмеженого доступу або камери безпеки, щоб запобігти несанкціонованому фізичному доступу.

9. Навчання та обізнаність: розкажіть користувачам про важливість безпеки портів і пристроїв, а також запропонуйте навчання щодо найкращих практик використання та захисту зовнішніх пристроїв. Користувачі повинні знати про ризики, пов’язані з підключенням невідомих або ненадійних пристроїв.

Впроваджуючи ці заходи, організації можуть ефективно керувати доступом до портів і пристроїв вводу/виводу, зменшуючи ризик несанкціонованого доступу, витоку даних і потенційної вразливості безпеки.

3. АНАЛІЗ ПОШУКОВИХ СИСТЕМ ЗЛАМАНИХ АКАУНТІВ

3.1 haveibeenpwned.com

Have I Been Pwned (HIBP) – це веб-сайт і служба, створені дослідником безпеки Троєм Хантом. Це дозволяє особам перевіряти, чи їх особиста інформація, наприклад адреси електронної пошти чи імена користувачів, була скомпрометована внаслідок витоку даних. Ось як працює Have I Been Pwned:

— Моніторинг витоків даних: HIBP постійно відстежує витоки загальнодоступних даних, які відбуваються в Інтернеті. Щоразу, коли виявляється порушення даних або повідомляється про нього, HIBP збирає пошкоджені дані та додає їх до своєї бази даних.

— Пошук скомпрометованих даних: користувачі можуть відвідати веб-сайт HIBP (haveibeenpwned.com) і ввести свою електронну адресу або ім’я користувача в полі пошуку. Потім HIBP перевірить, чи була ця інформація скомпрометована через будь-які відомі порушення даних.

— Повідомлення про порушення: якщо HIBP знайде відповідність введеній адресі електронної пошти чи імені користувача у своїй базі даних, він відобразить інформацію про порушення. Це включає інформацію про зламані веб-сайти чи служби, тип зламаних даних і дату порушення.

— Перевірка пароля: HIBP також надає функцію перевірки пароля, за допомогою якої користувачі можуть перевірити, чи їхні паролі були розкриті внаслідок витоку даних. Ця функція дозволяє користувачам перевіряти безпеку своїх паролів, не передаючи їх через Інтернет.

Важливо зауважити, що HIBP надає лише інформацію про загальновідомі порушення даних. Можуть бути витоку даних, які не включені в базу даних HIBP. Крім того, HIBP не зберігає повні адреси електронної пошти чи імена користувачів у своїй базі даних з міркувань конфіденційності. Натомість для порівняння використовується частковий хеш даних.

HIBP служить цінним інструментом для людей, щоб перевірити, чи їхня особиста інформація була скомпрометована, і вжити відповідних заходів, наприклад змінити паролі, увімкнути двофакторну автентифікацію та бути обережними щодо потенційних спроб фішингу. Це також допомагає підвищити обізнаність про поширеність витоку даних і важливість захисту особистої інформації в Інтернеті.

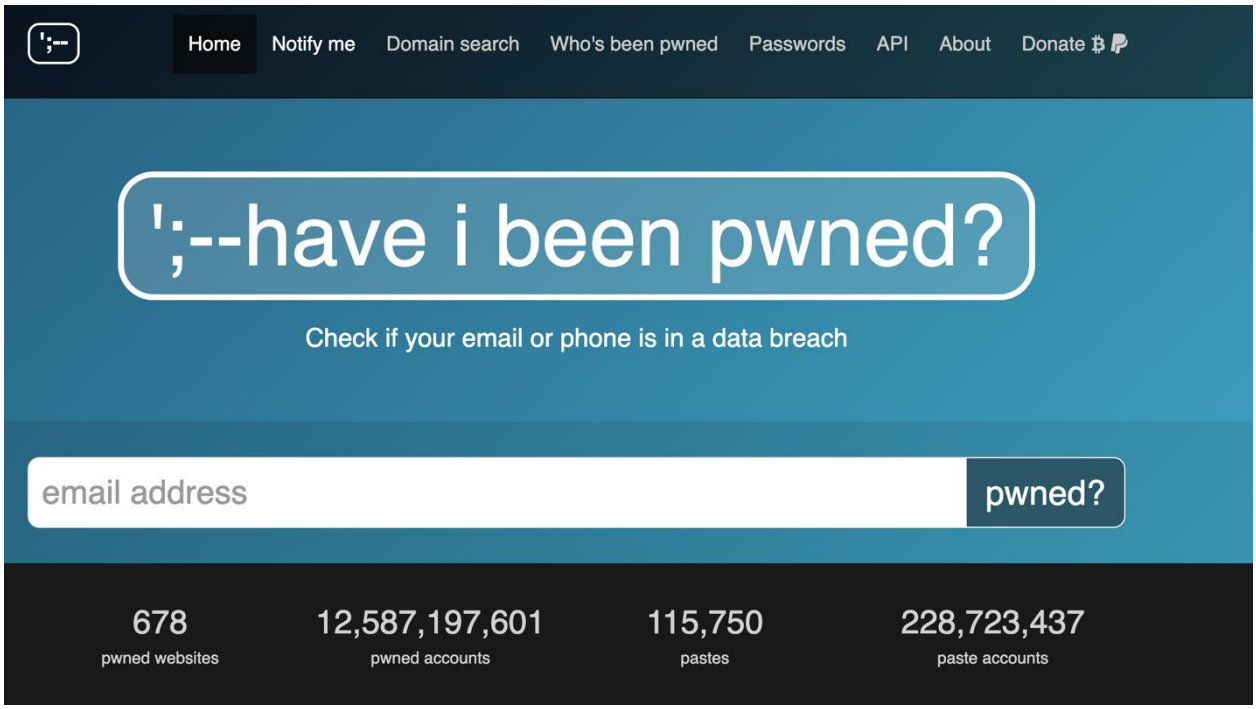

Рисунок 3.1 – Інтерфейс пошукової системи haveibeenpwned.com

3.2 Firefox Monitor

Firefox Monitor — це служба, яку надає Mozilla, організація, що стоїть за веб-браузером Firefox. Він розроблений, щоб допомогти людям відстежувати та захищати свої облікові записи в Інтернеті, сповіщаючи їх, якщо їх адреса електронної пошти з’являється під час відомого порушення даних. Ось як працює Firefox Monitor:

— Моніторинг адреси електронної пошти: користувачі можуть відвідати веб-сайт Firefox Monitor (monitor.firefox.com) і ввести свою адресу

електронної пошти, щоб розпочати процес моніторингу. Firefox Monitor безпечно перевіряє введену адресу електронної пошти за базою даних про відомі витоки даних.

— Сповіщення про порушення даних: якщо Firefox Monitor знайде відповідність введеній адресі електронної пошти у своїй базі даних відомих порушень, він надішле сповіщення користувачеві. У сповіщенні буде надано інформацію про зламаний веб-сайт або службу, тип зламаних даних і рекомендації щодо дій для захисту облікового запису.

— Кілька адрес електронної пошти: Firefox Monitor дозволяє користувачам відстежувати декілька адрес електронної пошти, забезпечуючи додатковий рівень захисту, відстежуючи ширший діапазон облікових записів.

Партнерство з Have I Been Pwned: Firefox Monitor співпрацює з Have I Been Pwned (HIBP), відомою службою повідомлень про порушення даних. Завдяки цьому партнерству Firefox Monitor використовує базу даних HIBP для надання інформації про відомі порушення.

Окрім повідомлень про порушення, Firefox Monitor надає рекомендації щодо покращення безпеки облікового запису. Це включає такі пропозиції, як увімкнення двофакторної автентифікації, використання надійних і унікальних паролів і регулярне оновлення паролів.

Firefox Monitor має на меті розширити можливості користувачів, надаючи їм інформацію про можливі порушення даних, пов’язані з їхніми електронними адресами. Негайно сповіщаючи людей про скомпрометовані облікові записи, Firefox Monitor дозволяє користувачам вживати проактивних заходів для захисту своєї онлайн-безпеки та конфіденційності.

Важливо зауважити, що Firefox Monitor покладається на загальнодоступну інформацію про витоки даних і може не мати повного охоплення всіх витоків. Тому рекомендується регулярно оновлювати паролі, використовувати надійні методи безпеки та відстежувати активність облікового запису в різних онлайн-сервісах.

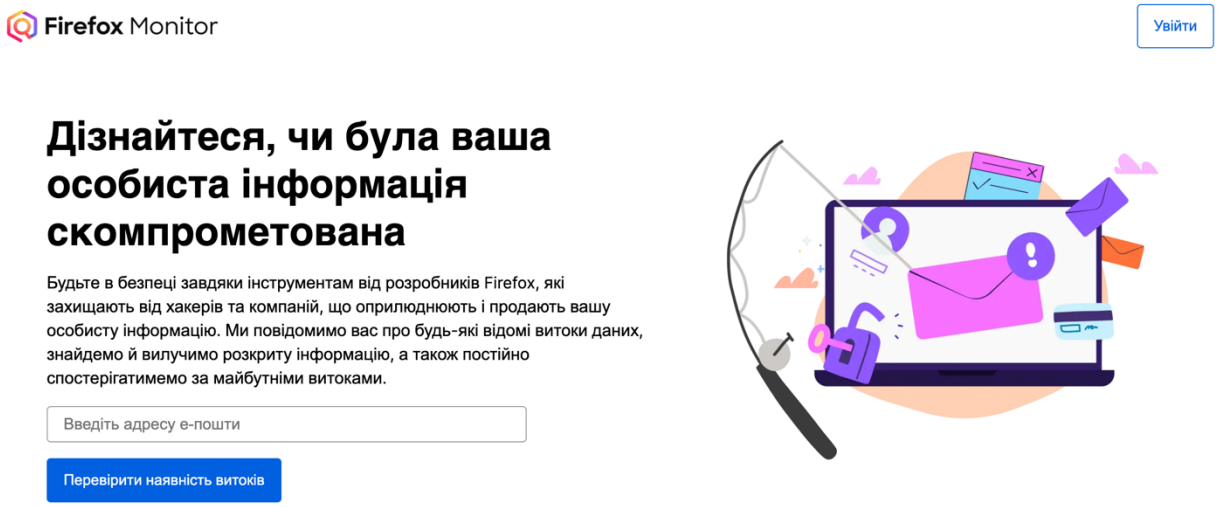

Рисунок 3.2 - Інтерфейс пошукової системи Firefox Monitor

3.3 Password Checkup

Password Checkup – це функція безпеки, розроблена Google, яка допомагає користувачам перевіряти безпеку своїх паролів. Він призначений для сповіщення користувачів, якщо їхні паролі було зламано внаслідок витоку даних, і спонукає їх вжити заходів для підвищення безпеки свого облікового запису. Перевірка пароля працює так:

— Аналіз паролів: коли користувачі входять у свій обліковий запис Google або використовують веб-браузер Chrome, Password Checkup автоматично аналізує паролі, які вони вводять, щоб перевірити, чи не зазнавали вони раніше порушень даних. Аналіз виконується локально на пристрої користувача, забезпечуючи конфіденційність його даних.

— Сповіщення про порушення: якщо Password Checkup виявляє, що пароль користувача було зламано в результаті порушення даних, відображається сповіщення з порадою користувача вжити заходів. Сповіщення містить інформацію про зламаний веб-сайт або службу та пропонує користувачеві змінити свій пароль.

— Допомога при зміні пароля: Password Checkup може допомогти

користувачам створити надійніший і безпечніший пароль, пропонуючи пропозиції та направляючи їх через процес зміни зламаного пароля. Це заохочує користувачів застосовувати більш надійні методи безпеки для своїх облікових записів.

— Інтеграція з обліковими записами Google: Password Checkup інтегровано в облікові записи Google і Chrome, що дозволяє користувачам переглядати статус безпеки своїх паролів у налаштуваннях облікового запису Google. Вони можуть переглянути зведення зламаних паролів і вжити заходів для захисту своїх облікових записів.

— Конфіденційність і безпека: Google наголошує на конфіденційності та безпеці даних користувачів за допомогою Password Checkup. Ця функція розроблена для роботи локально на пристрої користувача без передачі паролів Google або іншим зовнішнім серверам. Інформація про порушення хешується та шифрується для захисту конфіденційності користувачів.

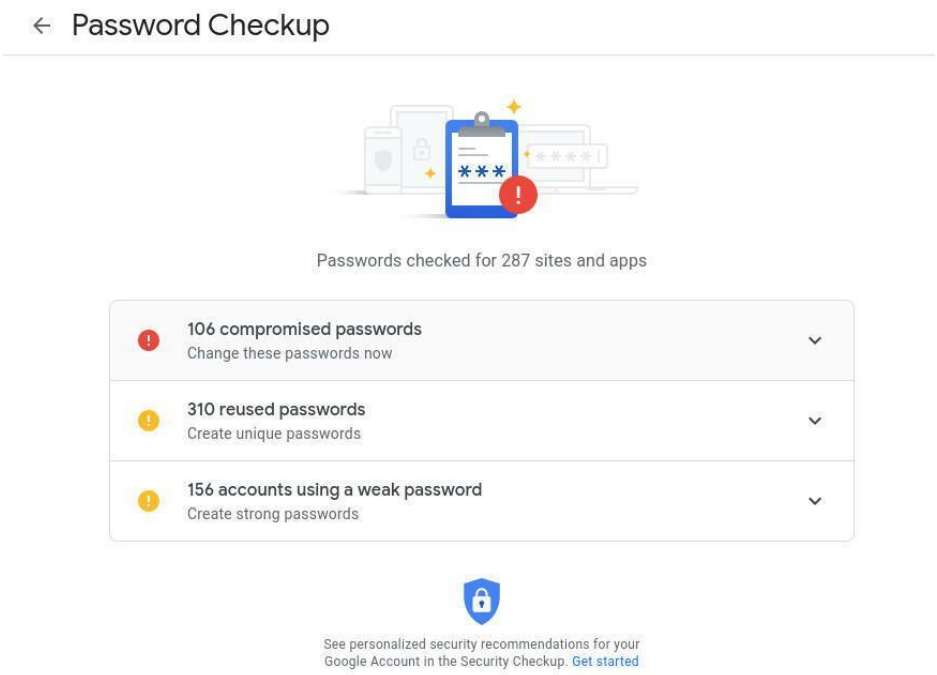

Рисунок 3.3 - Інтерфейс пошукової системи Password Checkup

Перевірка паролів є частиною зусиль Google, спрямованих на підвищення рівня безпеки та допомогу користувачам у захисті їхніх облікових записів в Інтернеті. Надаючи сповіщення про скомпрометовані паролі, він заохочує користувачів дотримуватися гігієни паролів і вживати заходів для захисту своєї цифрової особистості.

3.4 Sucuri Security Scanner

Sucuri Security Scanner — це веб-інструмент безпеки, наданий Sucuri, провідною компанією з кібербезпеки, що спеціалізується на захисті веб-сайтів і видаленні шкідливих програм. Сканер розроблений, щоб допомогти власникам веб-сайтів виявляти та усувати вразливості безпеки, зараження зловмисним програмним забезпеченням та інші потенційні загрози. Ось огляд Sucuri Security Scanner:

— Виявлення зловмисного програмного забезпечення: Sucuri Security Scanner сканує ваш веб-сайт на наявність відомих сигнатур зловмисного програмного забезпечення та підозрілих шаблонів коду. Це допомагає виявити зараження зловмисним програмним забезпеченням, яке може бути присутнім на вашому веб-сайті, зокрема бекдори, фішингові сторінки, шкідливі сценарії та інші типи шкідливого коду.

— Моніторинг чорного списку: Sucuri відстежує різні чорні списки, щоб перевірити, чи позначено ваш веб-сайт як зловмисний або скомпрометований. Це допомагає визначити, чи негативно вплинуло на репутацію вашого веб-сайту, що потенційно може призвести до штрафів або попереджень пошукової системи.

— Перевірка вразливості системи безпеки: Сканер перевіряє загальні вразливості безпеки на вашому веб-сайті, такі як застарілі версії програмного забезпечення, неправильні конфігурації, слабкі паролі та незахищені дозволи на файли. Виявлення цих вразливостей допоможе вам завчасно їх усунути та

покращити рівень безпеки вашого веб-сайту.

— Моніторинг цілісності веб-сайту: Сканер безпеки Sucuri містить функцію під назвою Моніторинг цілісності веб-сайту (WIM), яка відстежує зміни у файлах вашого веб-сайту та виявляє будь-які неавторизовані зміни. Це допомагає визначити, чи ваш веб-сайт було підроблено, що вказує на потенційне порушення безпеки.

— Рекомендації щодо безпеки: на основі результатів сканування Sucuri надає рекомендації щодо безпеки та вказівки щодо вирішення виявлених проблем. Це може включати кроки з видалення зловмисного програмного забезпечення, оновлення програмного забезпечення, посилення контролю доступу та підвищення загальної безпеки веб-сайту.

— Інформаційна панель і звітність: Sucuri пропонує зручну інформаційну панель, на якій можна переглядати результати сканування, контролювати стан безпеки вашого веб-сайту та отримувати доступ до детальних звітів. Це дозволяє відстежувати покращення безпеки з часом і бути в курсі будь-яких потенційних проблем.

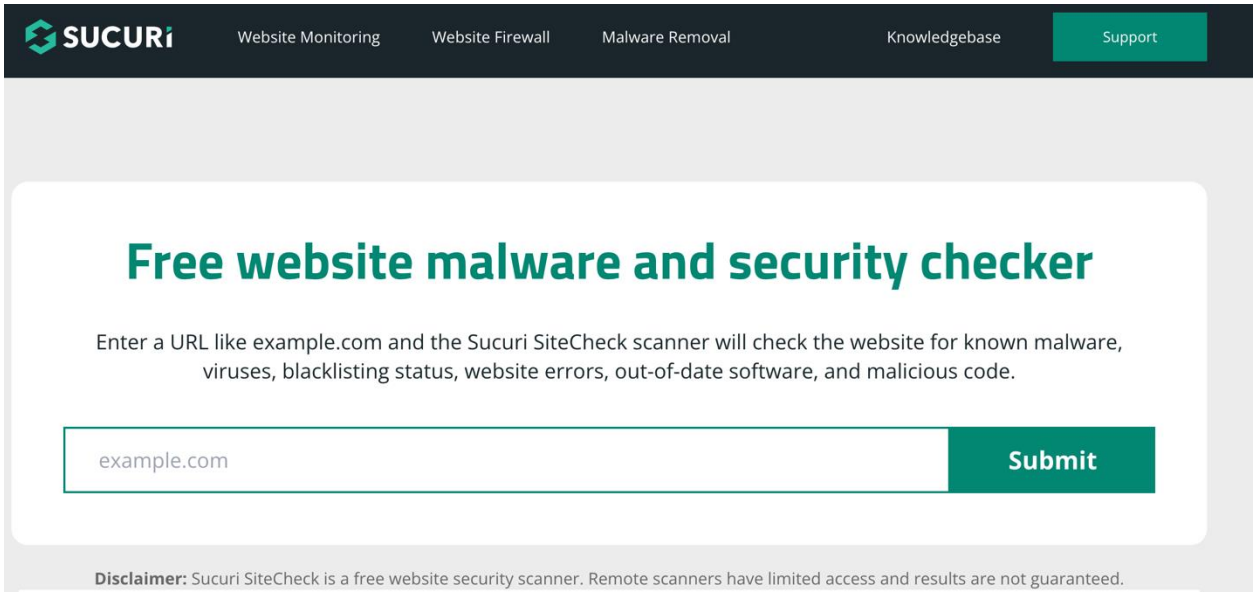

Рисунок 3.4 - Інтерфейс пошукової системи Sucuri Security Scanner

Sucuri Security Scanner є одним із компонентів ширшого набору служб

безпеки веб-сайтів Sucuri, який також включає захист веб-сайту брандмауером, пом'якшення DDoS та служби реагування на інциденти. Важливо зауважити, що хоча сканер може допомогти виявити типові проблеми безпеки, він не гарантує повного захисту від усіх можливих загроз. Регулярне технічне обслуговування безпеки, оновлення та передові методи все ще є важливими для підтримки безпечного веб-сайту.

3.5. Практична реалізація та застосування запитів до пошукових систем

На фрагменті коду, який зображено на рисунку 3.5, можна бачити, що введено змінні для підключення API від HIBP та Intelx, а також власні дані з Telegram, для використання боту з пошуку витоків паролів за електронною адресою.

Рисунок 3.5 – Фрагмент коду програми

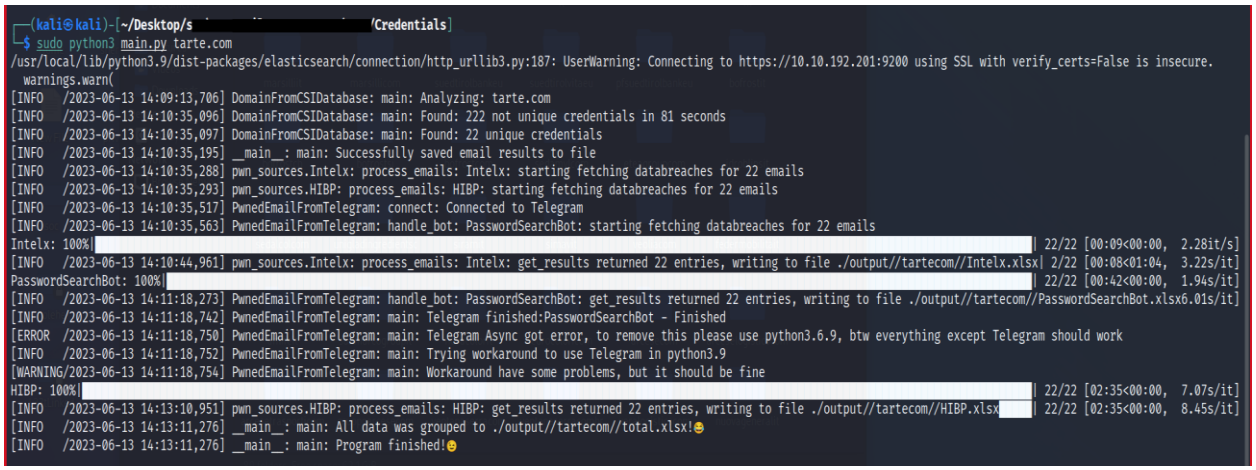

Рисунок 3.6 – Результат пошуку програми за доменом tarte.com

Введення таких змінних є корисним, адже кожен, хто захоче використовувати програму може без проблем швидко змінювати дані, а також у тих випадках, коли наші підключені безкоштовні API мають певні обмеження по кількості безкоштовних пошуків.

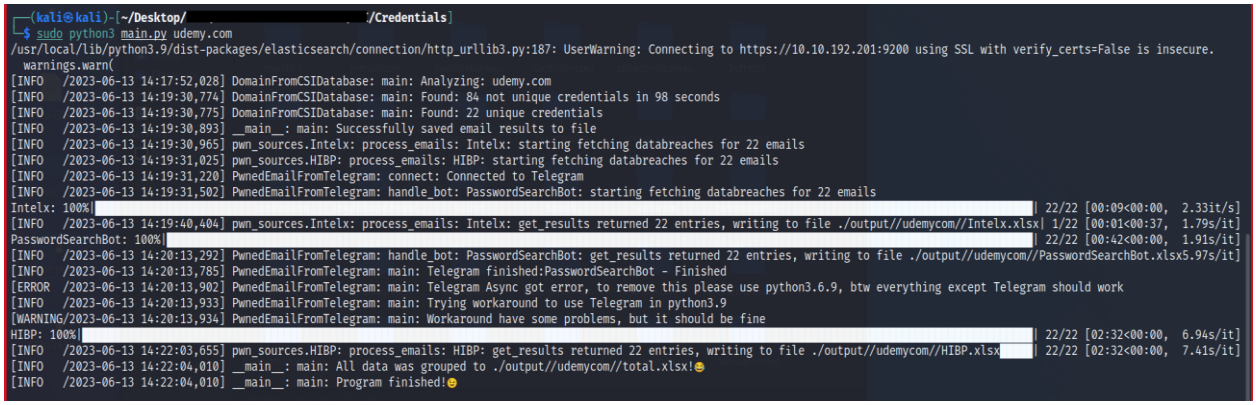

Рисунок 3.7 – Результат пошуку програми за доменом udemy.com

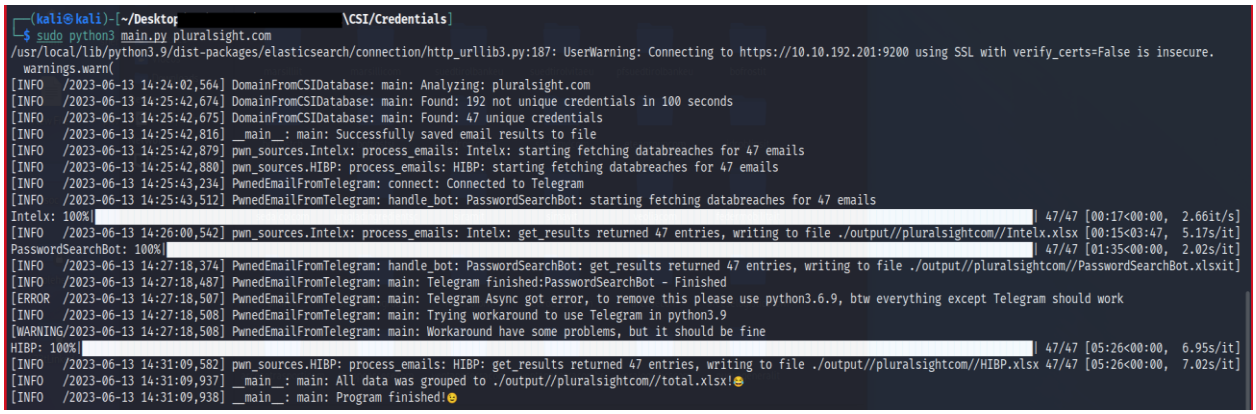

Рисунок 3.8 – Результат пошуку програми за доменом pluralsight.com

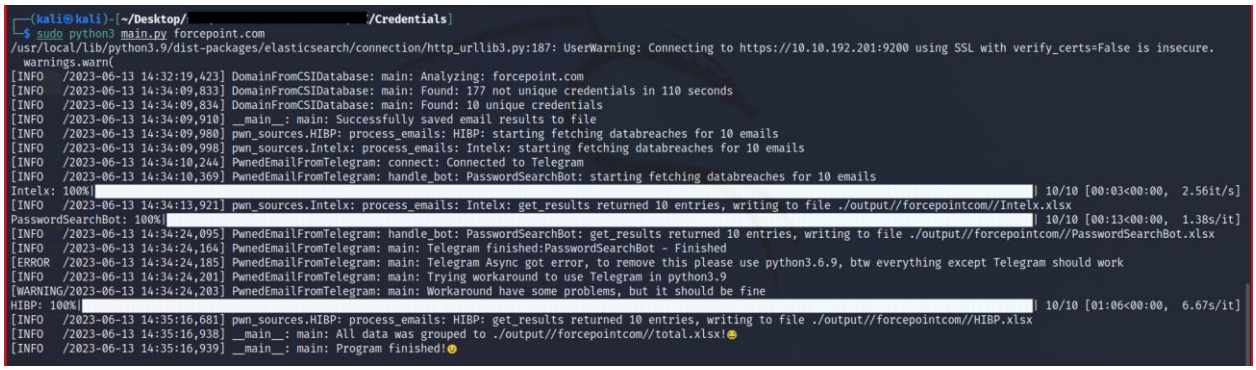

Рисунок 3.9 – Результат пошуку програми за доменом forcepoint.com

На рисунках 3.6, 3.7, 3.8, 3.9 бачимо результат пошуку за доменами tarte.com , udemy.com, pluralsight.com та forcepoint.com.

	Email	Compromised in data breach	Password(s)	Databreach Name
0	casey@tarte.com	TRUE	7b4076e17809ac 267401428e408c 8d98bd0aed06 password	CompilationOfManyBreaches MGM2022Update, BreachDate: 2019-07-25 ExploitIn, BreachDate: 2016-10-13 Dropbox.com Collection #1_EU combos ANTIPUBLIC #1 Collection1, BreachDate: 2019-01-07 Collection #2_New combo cloud_General Splits Collection Dropbox, BreachDate: 2012-07-01 Collection #2_New combo cloud_Money Related Collection
1	janice@tarte.com	TRUE	JaniceTarte	AntiPublic, BreachDate: 2016-12-16 CompilationOfManyBreaches Collection #2_New combo cloud_Private Collection Collection #2_New combo cloud_Private Collection_xeee Collection #4_EU COMBOS_Разбитая база 03 11 00-05-57 ExploitIn, BreachDate: 2016-10-13 Collection #1_EU combos ANTIPUBLIC #1 Collection #4_Goods Collection #4_Update combos Collection1, BreachDate: 2019-01-07 Collection #2_New combo cloud_General Splits Collection Collection #2_New combo cloud_Money Related Collection
2	tata@tarte.com	TRUE	6554	AntiPublic, BreachDate: 2016-12-16 CompilationOfManyBreaches ANTIPUBLIC #1 OnlinerSpambot, BreachDate: 2017-08-28 Collection #2_New combo cloud_General Splits Collection iMesh, BreachDate: 2013-09-22

Рисунок 3.10 – Перелік скомпроментованих акаунтів за доменом tarte.com

	Email	Compromised in data breach	Password(s)	Databreach Name
0	email@udemy.com	TRUE	emailudemy	Collection #1_NEW combo semi private_Private combos Collection #2_New combo cloud_Private Collection_Private combos CompilationOfManyBreaches Collection #2_New combo cloud_UPDATES_Update 24 11 2018 Collection1, BreachDate: 2019-01-07
2	jeff@udemy.com	TRUE	jeff	Collection #4_EU + RUSSIAN COMBOS Collection #2_New combo cloud_VIP Collection_More Lists CompilationOfManyBreaches
3	marc@udemy.com	TRUE	udemy12 0b4c3914356ff8c8ad7d817e ae0e41b4	Cit0day, BreachDate: 2020-11-04 past.internet-librarian.com {32.373} [HASH+NOHASH] (Education)_special_for_XSS.IS
4	adam@udemy.com	TRUE	4e1cbd77ffb232ba4f169b1b e62604f1	PDL, BreachDate: 2019-10-16 Gravatar, BreachDate: 2020-10-03 YouveBeenScraped, BreachDate: 2018-10-05 Apollo, BreachDate: 2018-07-23 Appen, BreachDate: 2020-06-22 Cit0day, BreachDate: 2020-11-04 db8151dd, BreachDate: 2020-02-20 VerificationsIO, BreachDate: 2019-02-25 pharmready.com {1.008} [HASH] (Medicine)_special_for_XSS.IS Adapt, BreachDate: 2018-11-05

Рисунок 3.11 – Перелік скомпроментованих акаунтів за доменом udemy.com

23	21	Catherine-stenson@pluralsight.com	TRUE	9719003e598a4f81bf9c3b45c14d847ee425bdd3	Canva, BreachDate: 2019-05-24 lemondeinformatique.fr {150.536} [HASH+NOHASH] (IT)_special_for_XSS.IS Apollo, BreachDate: 2018-07-23 8fit, BreachDate: 2018-07-01 Cit0day, BreachDate: 2020-11-04
24	22	jc-dejongh@pluralsight.com	TRUE	26e8e69ad9fd6410ec20c081a7fdf4b0a71af126	LinkedInScrape, BreachDate: 2021-04-08 Adapt, BreachDate: 2018-11-05 lemondeinformatique.fr {150.536} [HASH+NOHASH] (IT)_special_for_XSS.IS Cit0day, BreachDate: 2020-11-04 PDL, BreachDate: 2019-10-16
25	23	christina-robohm@pluralsight.com	TRUE	talent2575	Cit0day, BreachDate: 2020-11-04 talentsmart.com {105.545} [NOHASH] (Education)_special_for_XSS.IS
26	24	david@pluralsight.com	TRUE	6d0ccf24ec0e58aa7634c75e47b61635e2d06534	Adapt, BreachDate: 2018-11-05 VerificationsIO, BreachDate: 2019-02-25 Apollo, BreachDate: 2018-07-23 Dropbox.com PDL, BreachDate: 2019-10-16 Dropbox, BreachDate: 2012-07-01
					Adapt, BreachDate: 2018-11-05 YouveBeenScraped, BreachDate: 2018-10-05 VerificationsIO, BreachDate: 2019-02-

Рисунок 3.12 – Перелік скомпроментованих акаунтів за доменом pluralsight.com

За результатами цього пошуку знайдено 22 злиті електронні пошти, які належать доменам tarte.com та udemy.com, 47 злитих електронних пошт за доменом pluralsight.com та 10 електронних пошт за доменом forcepoint.com. Після того, як було виявлено, що ці електронні належать деяким дата брічам, проводиться пошук паролів цих електронних адрес в телеграм-боті і ці всі знайдені дані записуються в вихідний Excel-файл.

			pofyqo	AntiPublic, BreachDate: 2016-12-16
			xZjZlc5jaw==	Cit0day, BreachDate: 2020-11-04
			catch2235	Apollo, BreachDate: 2018-07-23
			$2a$08$zYCvtgI8p	Collection #2_New combo cloud_Shopping Collection
			PmlyHMF1PqKD.yR	Collection #4_EU COMBOS_Разбитая база 03 11 00-05-57
			mnEF6HGwkssp3/y	Dropbox, BreachDate: 2012-07-01
			MneqRwFhAHrXXm	2844Breaches, BreachDate: 2018-02-19
			xZjZlc5jaw	playsanctum.net {60.308} [NOHASH] (IT)_special_for_XSS.IS
			abcd1234	Collection #2_New combo cloud_Database Collection_Dump
1	wbackes@forcepoint.com	TRUE	catch22	расшифрованные
				Collection1, BreachDate: 2019-01-07
			32853831ebc1405	Collection #2_New combo cloud_UPDATES_November 4th
			5d7a0351c7bcea0	2018_Update Dumps
2	mnazim@forcepoint.com	TRUE	51	Collection #1_NEW combo semi private_Update Dumps
				Cit0day, BreachDate: 2020-11-04
	heather.berggren@forcepoin		9acfe53e16f07ff4f3	cisosonthemove.com {6.363} [HASH+NOHASH]
3	t.com	TRUE	878baa3f41c0e6	(Business)_special_for_XSS.IS
				Cit0day, BreachDate: 2020-11-04
				Apollo, BreachDate: 2018-07-23
				Adapt, BreachDate: 2018-11-05
				emarketingparis.com {107.847} [NOHASH]
				(Business)_special_for_XSS.IS
4	vmaupou@forcepoint.com	TRUE	FP2016	PDL, BreachDate: 2019-10-16
				Cit0day, BreachDate: 2020-11-04
				LinkedInScrape, BreachDate: 2021-04-08
				MGM2022Update, BreachDate: 2019-07-25
			3d0648fb3016336	sheshcykamd5 {482.602} [HASH+NOHASH]
			ca047241fa724c72	(NoCategory)_special_for_XSS.IS
			c	myhotelbb.it {2.875} [HASH+NOHASH] (IT)_special_for_XSS.IS
5	baiana@forcepoint.com	TRUE	Poppina11	PDL, BreachDate: 2019-10-16

Рисунок 3.13 – Перелік скомпроментованих акаунтів за доменом forcepoint.com

4. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1. Долікарська допомога при задусі, утопленні

Перша долікарська допомога – це комплекс найпростіших, термінових та необхідних дій, які проводяться до прибуття лікаря чи доставлення потерпілого в медичний заклад і спрямовані на відновлення та збереження його життя та здоров'я. [10]. Такий вид допомоги існує у вигляді самодопомоги (потерпілий надає долікарську допомогу сам собі) та взаємодопомоги (допомогу надає особа, яка перебуває поряд із потерпілим).

Перш ніж надавати долікарську допомогу собі або потерпілому, варто зберігати спокій та не піддаватися паніці, оскільки такі дії можуть мати негативний вплив на подальші кроки та лише загострити ситуацію. Людина, яка надає допомогу, повинна бути уважною та обережною щодо середовища, у якому перебуває вона та потерпілий, а також щодо знань домедичних дій, які планує виконати. Вона має пам'ятати загальні принципи надання першої долікарської допомоги відповідно до характеру виявлених пошкоджень.

Задуха або асфіксія – припинення надходження кисню в легені протягом 2-3 хв. Зупиняється газообмін в легенях, настає кисневе голодування, людина непритомніє [11]. Внаслідок цього настає зупинка серця, що призводить до смерті потерпілого. Асфіксія може виникнути внаслідок фізичного стискання гортані і трахеї рукою або іншими предметами, потраплянню чужорідного предмету в дихальні шляхи, заповнення водою дихальних шляхів, отруєння токсичними речовинами тощо. Може супроводжуватися блювотинням або слизовими масами. Утоплення – це один із видів механічної асфіксії, де механічним фактором, що спричиняє це явище, є будь-яка рідина, що заповнила дихальні шляхи.

Зокрема перед тим, як надавати першу допомогу при задусі чи утопленні, людина-рятувальник повинна вміти:

— оцінити стан потерпілого (наявність свідомості, ритм дихання, серцеві скорочення, розмір зіниць, колір шкіри тощо).

— оцінити характер пошкоджень, на основі чого визначити свої наступні кроки у наданні допомоги;

— користуватися аптечкою швидкої допомоги, оцінювати її вміст та використовувати препарати відповідно до характеру пошкодження;

— забезпечити прохідність верхніх дихальних шляхів при задусі (застосування прийому Геймліха);

— виконувати штучне дихання «із рота в рот / ніс» та зовнішній масаж серця;

— використовувати підручні засоби для транспортування потерпілого у разі потреби;

— визначати необхідність перевезення потерпілого власним авто або машиною швидкої допомоги.

Перед тим як надавати долікарську допомогу утопленику варто оцінити всі ризики, оскільки потерпілий не контролює свої дії у стані шоку. Він може схопити рятівника за руки або шию, обмеживши не лише у діях, але й спричинивши ще більшу загрозу життю для обох. До утопленика потрібно підпливати ззаду, схопити за волосся або під пахви, обернути обличчям догори та пливти у сторону берега. Щойно потерпілий опиниться на суші, негайно застосовують першу домедичну допомогу. Пальцями або куском тканини (за наявності) видаляють зайві предмети з порожнини рота, наприклад, пісок, водорості та інше. Для того, щоб усунути воду з дихальних шляхів, рятувальник стає на одне коліно, кладе утопленика животом на стегно другої ноги так, щоб голова та плечі потерпілого були опущеними (рис. 4.1.). Тоді кілька разів натискує руками в одному темпі на спину. Коли з дихальних шляхів утопленика витече вода та верхні дихальні шляхи стануть вільними, потерпілого кладуть обличчям догори. Якщо дихання відсутнє – проводять штучну вентиляцію легень, а при зупинці серця – непрямий масаж серця.

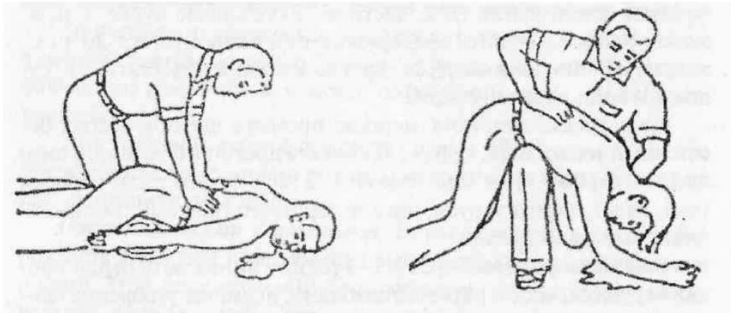

Рисунок 4.1 - Видалення води з дихальних шляхів і шлунка потерпілого

Механічна асфіксія супроводжується такими симптомами як посиніння обличчя, кашель, різка зміна артеріального тиску, звуження й розширення зіниць, втрата свідомості. Перша долікарська допомога при задусі від чужорідного предмета передбачає застосування прийому Геймліха. Для цього потрібно стати позаду потерпілого у положенні стоячи, стиснути один кулак і покласти його на нижню половину грудини. Кулак обхопити іншою рукою. Одночасно потягнувши дві руки до себе здійснити різкі поштовхи 6-10 разів (рис 4.2).

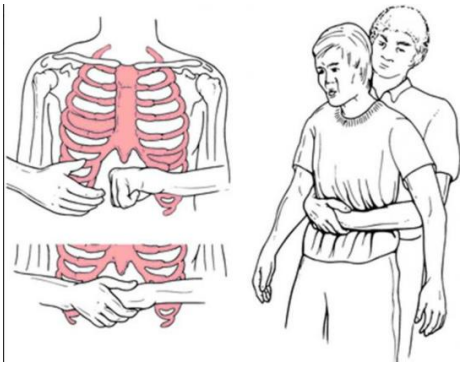

Рисунок 4.2 - Використання прийому Геймліха при задусі у положенні стоячи

Отже, важливість надання долікарської допомоги полягає в тому, що вона зменшує ризики негативних наслідків для потерпілого від задухи чи утоплення до прибуття швидкої допомоги. Кожен повинен опанувати прості техніки, які можуть врятувати своє чи життя іншої людини у

непередбачуваних ситуаціях. Тож особисте знання та вміння надавати домедичну допомогу мають величезне значення для збереження життя.

4.2. Засоби особистої гігієни працюючих

Засоби особистої гігієни є невід'ємною частиною дотримання умов праці та забезпечення здоров'я працюючих на підприємстві. Перед влаштуванням на роботу на дільницю цеху майбутній працівник зобов'язаний пройти медичне обстеження, а згодом періодичний медичний огляд. Результати обстеження заносяться в особову медичну книжку, що дає право на допуск до роботи. Якщо в особи були виявлені інфекційні хвороби, то її направляють на лікування або санацію. Допуск такої особи до роботи проводиться тільки за наявності довідки лікувально-профілактичного закладу про видужання.

Керівники підприємств та організацій зобов'язані надати працівникам засоби індивідуального захисту та особистої гігієни відповідно до характеру виробництва та умов праці. Необхідно забезпечити доступність та належний стан засобів особистої гігієни, а також надавати необхідну інформацію та інструктаж щодо їх правильного використання задля збереження здоров'я та запобігання виробничим захворюванням.

Одним з головних засобів особистої гігієни є миття рук перед початком роботи, після контакту зі забрудненими матеріалами, а також перед прийомом їжі та після відвідування туалету. В інструкції з впровадження покращення гігієни рук в закладах охорони здоров'я та установах / закладах надання соціальних послуг / соціального захисту населення зазначено обов'язкове забезпечення працівників необхідними засобами для миття рук, такими як рідке мило та вода, одноразові паперові рушники та антисептичними засобами для дезінфекції рук [12].

Окрім цього, умови роботи на підприємстві можуть включати контакт зі шкідливими речовинами, пилом або іншими небезпечними факторами. У таких випадках працівники повинні мати доступ до відповідних засобів індивідуального захисту. Наприклад, до респіраторів типу N95 або FFP2 для захисту від шкідливих частинок, пилу, аерозолей, диму та інших забруднюючих речовин, які можуть бути присутніми на підприємстві, або до захисних окулярів від розпилення рідин або іскор. Використання цих засобів допомагає запобігти вдиханню шкідливих речовин та захистити органи чуття та дихальні шляхи працівників.

Додатково, умови роботи на підприємстві можуть вимагати засобів гігієни тіла. Зокрема це можуть бути душові кабіни та засоби для миття, як-то мило, шампунь та гель для душу. Вони дають змогу працівникам змити з себе бруд та забруднення, а також зменшують ризик поширення інфекцій.

Важливим аспектом забезпечення гігієни під час робочого процесу є правильна утилізація відходів, пов’язаних з особистою гігієною працівників. Керівники дільниць цехів мають забезпечити працівникам належні умови збирання та утилізації відходів, таких як використані рукавички, маски або інші одноразові засоби. Зокрема це можуть бути спеціальні контейнери для утилізації.

Отже, дотримання визначених санітарних норм на підприємстві та забезпечення належної особистої гігієни має безпосередній вплив на здоров'я та безпеку працівників, а також на якість та продуктивність робочого процесу загалом. Чистота робочого середовища та зменшення контакту зі шкідливими речовинами допомагають знизити ризик розвитку професійних захворювань та покращити самопочуття працівників.

ВИСНОВКИ

В цій кваліфікаційній роботі було вивчено та досліджено основні факти та шляхи витоку інформації в компаніях, а також заходи, які можна вжити для запобігання цим витокам. Були розглянуті такі аспекти, як витікаючий веб-трафік, контроль доступу до пристроїв та портів введення-виведення, а також інші методи попередження витоку даних.

Для досягнення поставлених цілей, в рамках цієї роботи було створено власний інструмент з використанням мови програмування Python. Цей інструмент допомагає проводити аналіз доменів компаній і виявляти витоки даних, пов'язані з цими доменами.

Аналіз витоків даних у великих організаціях та методи їх попередження мають надзвичайну важливість у сучасному світі. Зростаюча кількість компаній зберігають і обробляють значну кількість конфіденційних даних, включаючи особисту інформацію клієнтів, фінансові дані та комерційні таємниці. Виток таких даних може призвести до серйозних наслідків, включаючи фінансові втрати, порушення конфіденційності та втрату довіри клієнтів. Зростання кількості кібератак і супутніх загроз демонструє необхідність постійного аналізу та попередження витоків даних.

Таким чином, розвиток ефективних методів та інструментів для аналізу витоків даних та їх попередження стає все більш важливим завданням в майбутньому. Постійне вдосконалення заходів безпеки і розробка нових технологій для виявлення та запобігання витокам даних є ключовими аспектами для забезпечення захисту інформації великих організацій та збереження їх довіри клієнтів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bruce Schneier. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. 2015. c.97

2. Розподіл організацій, на яких націлений фішинг, за категоріями URL: https://www.kaspersky.com/about/press-releases/2023_the-number-of-phishing-attacks-doubled-to-reach-over-500-million-in-2022

3. Sherri Davidoff. Data Breaches: Crisis and Opportunity. 2019. c.23.

4. P.W. Singer, Allan Friedman. Cybersecurity and Cyberwar: What Everyone Needs to Know. 2013. c.73

5. Kevin Poulsen. Kingpin: How One Hacker Takok Over the Billion Dollar Cybercrime Underground. 2011. c.15

6. David Gourley, Brian Totty, Marjorie Sayer, Anshu Aggarwal, Sailu Reddy. HTTP: The Definitive Guide (Definitive Guides). 2002. c.49.

7. Scott Allen. HTTP Succinctly. 2017. c.6.

8. Steve Rackley. Understanding FTP: The Definitive Guide. 2019. c.174.

9. Туровська Г. І, Риженко І. М. Надання першої долікарської допомоги потрепілому. Методичні вказівки до виконання практичної роботи з дисципілни «Безпеки життєдіяльності» для студентів за всіма напрямами підготовки НУВГП денної та заочної форми навчання. – Рівне: НУВГП, 2012. С. 5

10. Долікарська допомога при задусі, утопленні, заваленні землею, отруєнні. URL: https://wikipage.com.ua/1x6984.htmlhttps://wikipage.com.ua/1x6984.html

11. Непритомність та колапс: причини виникнення, механізм розвитку, невідкладна допомога. URL: https://studies.in.ua/dolikarska-dopomoga/3970-nepritomnst-ta-kolaps-prichini-viniknennya-mehanzm-rozvitku-nevdkladna-dopomoga.html

12. Інструкція з впровадження покращення гігієни рук в закладах охорони здоров’я та установах/закладах надання соціальних послуг/ соціального захисту населення: наказ Міністерства охорони здоров’я України від 03.09.2021 р. № 1614

ДОДАТОК А
Функція пошуку в телеграм боті

```
BOTS = {
'PasswordSearchBot': lambda email: f'{email}',
}


def get_bot_message(bot_name: str, email: str) -> str():
"""
by bot name return the message that should be sent to bot to
start querying about leak
"""
return BOTS.get(bot_name, lambda x: f'{x}')(email)


def parse_response(message: str) -> List[str]:
"""
parse key points from bot responses
"""
patterns = [
            r'Name: (?P<Name>.+)\s.+\s.+BreachDate:
            (?P<Date>.+)\s',
            r'(?P<email>.+):(?P<password>.+)'
]

for pattern in patterns:
            match = [m.groupdict() for m in
            re.finditer(pattern, message)]
            if match:
            return [
                  True,
                  [m.get('password', '') for m in match if
                  m.get('password', False)],
                  [f"{m.get('Name', '')}, BreachFate:
                  {m.get('Date', '')}" for m in match if
                  m.get('Name', False)],
            ]
return [False, [], []]
```